# Installation and User Manual

**VideoEdge NVR**
Version 4.2.1

Part Number: 8200-0959-01 B0

## Notice

The information in this manual was current when published. The manufacturer reserves the right to revise and improve its products. All specifications are therefore subject to change without notice.

## Copyright

Under copyright laws, the contents of this manual may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine-readable form, in whole or in part, without prior written consent of Tyco International Ltd © 2011 and its Respective Companies. All Rights Reserved.

American Dynamics

6600 Congress Avenue

Boca Raton, FL 33487 U.S.A.

## Customer Service

Thank you for using American Dynamics products. We support our products through an extensive worldwide network of dealers. The dealer through whom you originally purchased this product is your point of contact if you need service or support. Our dealers are empowered to provide the very best in customer service and support. Dealers should contact American Dynamics at (800) 507-6268 or (561) 912-6259 or on the Web at www.americandynamics.net.

## Trademarks

Windows® is a registered trademark of Microsoft Corporation. PS/2® is a registered trademark of International Business Machines Corporation.

The trademarks, logos, and service marks displayed on this document are registered in the United States [or other countries]. Any misuse of the trademarks is strictly prohibited and Tyco International Ltd. will aggressively enforce its intellectual property rights to the fullest extent of the law, including pursuit of criminal prosecution wherever necessary. All trademarks not owned by Tyco International Ltd. are the property of their respective owners, and are used with permission or allowed under applicable laws.

Product offerings and specifications are subject to change without notice. Actual products may vary from photos. Not all products include all features. Availability varies by region; contact your sales representative.

## MPEG-4 Disclaimer

This product is licensed under the MPEG-4 Visual Patent Portfolio License for the personal and non-commercial use of a consumer to (i) encoding video in compliance with the MPEG-4 visual standard (“MPEG-4 Video”) and/or (ii) decoding MPEG-4 video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed by MPEG LA to provide MPEG-4 video. No license is granted or shall be implied for any other use. Additional information including that relating to promotional, internal and commercial uses and licensing may be obtained from MPEG LA, LLC. See HTTP://WWW.MPEGLA.COM

## H.264 Disclaimer

This product is licensed under the AVC Patent Portfolio License for the personal and non-commercial use of a consumer to (i) encode video in compliance with the AVC Standard (“AVC Video”) and/or (ii) decode AVC video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed to provide AVC video. No license is granted or shall be implied for any other use. Additional information may be obtained from MPEG LA, LLC. See HTTP://WWW.MPEGLA.COM

# Table of Contents


## Overview of the VideoEdge NVR

NVR Introduction . . . . . 1
Purpose of the NVR . . . . . 1
victor Digital Video Management System . . . . . 1
Getting Started with VideoEdge NVR . . . . . 2

## System Specifications

Overview . . . . . 5
System Specifications . . . . . 5
System Specifications for Bundled Packages . . . . . 5
Recommended System Specifications for Software Only . . . . . 6

## Installing the VideoEdge NVR

Overview . . . . . 7
NVR Hardware and Software Bundle . . . . . 7
NVR Software Only Bundle . . . . . 7
Installing the NVR Hardware and Software Bundle . . . . . 7
Initial Boot Up of the NVR . . . . . 8
Logging into the NVR Desktop . . . . . 10
Installing the NVR Software Only Bundle . . . . . 10
Verify the BIOS Configuration . . . . . 11
Boot your Computer/Server Using the NVR Software CD or USB . . . . . 11
Configure the NVR's System Information Settings . . . . . 12
Configure Storage Partitions . . . . . 13
Verify the Boot Loader location . . . . . 17
System Reboot After Basic Installation . . . . . 21
Set Up NVR OS User Accounts . . . . . 22
Log into the NVR Desktop . . . . . 24
VideoEdge Setup Wizard . . . . . 25
Accessing the Setup Wizard . . . . . 26

Preparation . . . . . 27
Welcome Page . . . . . 27
Setup Page . . . . . 27
Failover Page . . . . . 29
System . . . . . 30
System Info Page . . . . . 30
Roles Page . . . . . 31
Network . . . . . 32
Network General Page . . . . . 32
LAN Interface Page . . . . . 34
WAN Settings Page . . . . . 36
Dynamic Bandwidth Page . . . . . 37
DHCP Server Page . . . . . 38
Cameras . . . . . 40
Discovery Page . . . . . 40
Camera List Page . . . . . 41
Alarms Page . . . . . 42
Storage . . . . . 43
Basic Page . . . . . 44
Storage Sets Page . . . . . 45
Assign Cameras Page . . . . . 46
Email Alerts . . . . . 47
Email Alerts Page . . . . . 48
Finish . . . . . 49
Summary Page . . . . . 49

## Using the NVR Interface

Overview . . . . . 51
Logging into the NVR Server Web Interface . . . . . 51
victor NVR Configuration Interface . . . . . 52
**Navigating the NVR Interface . . . . . 54**
Live Video Menu . . . . . 55
Cameras Menu . . . . . 55
Storage Menu . . . . . 55
System Menu . . . . . 55
Network Menu . . . . . 56
Advanced Menu . . . . . 56

## Configuring Storage

Overview . . . . . 59
Overview of Storage Sets . . . . . 59
Verifying Storage Devices . . . . . 60
Basic Storage Configuration . . . . . 60

Enabling Media Folders for Storage . . . . . 61
Disabling Storage Media Folders . . . . . 62
Allocating Storage Space for Media . . . . . 63
Data Culling . . . . . 63
Vaulted Media . . . . . 64
Vault Media Quota . . . . . 64
Advanced Storage Configuration . . . . . 65
Creating Storage Sets . . . . . 67
Storage Set Recommendations . . . . . 67
Media Folder Assignment for Storage Sets . . . . . 68
Assigning Cameras to Storage Sets . . . . . 68
Calibrating Cameras . . . . . 69
Deleting Storage Sets . . . . . 70
Storage Statistics . . . . . 71
Storage Monitoring . . . . . 71

## Live Video

Overview . . . . . 73
Viewing Live Video . . . . . 73
Viewing Live Video with QuickTime . . . . . 75

## Camera List

Overview . . . . . 77
Viewing the Camera List . . . . . 79
Sorting the Camera List . . . . . 79
Filtering the Camera List . . . . . 79
Manually Adding an IP Camera or Encoder . . . . . 80
Adding Cameras Using Auto-Discovery . . . . . 82
Removing a Camera . . . . . 84

## Camera Configuration

Overview . . . . . 85
Basic Camera Configuration . . . . . 85
Batch Camera Configuration . . . . . 86
Advanced Camera Configuration . . . . . 89
Configuring General Camera Settings . . . . . 90

Edit a Camera Name . . . . . 90
Change the Password Group Assigned to an IP Camera . . . . . 91
Change a Camera's Storage Set . . . . . 91
Configure Camera Image Settings . . . . . 92
Configure Camera Function and Stream Settings . . . . . 93
Set the Camera Recording Status . . . . . 95
Set a Camera Recording Retention Period . . . . . 96
Configuring Camera Audio Settings . . . . . 96
Configuring Camera Stream Settings . . . . . 97
Configuring Alert Buffer Settings . . . . . 98
Configuring Sensors . . . . . 99
Dry Contact Sensors . . . . . 99
Configuring PTZ Settings . . . . . 100
Enable/Disable PTZ Functionality . . . . . 100
Return to Home . . . . . 101

## Motion Detection

Overview . . . . . 103
Motion Detection Best Practices . . . . . 103
Enabling Motion Detection . . . . . 104
Disabling Motion Detection . . . . . 106
Motion Detection Alarms . . . . . 106
Creating a Motion Detection Camera Alarm . . . . . 108
Editing a Motion Detection Camera Alarm . . . . . 110
Disabling a Motion Detection Camera Alarm . . . . . 110
Deleting a Motion Detection Camera Alarm . . . . . 111

## Video Intelligence

Overview . . . . . 113
Video Intelligence Best Practices . . . . . 114
Enable Video Intelligence for a Camera . . . . . 115
Disable Video Intelligence for a Camera . . . . . 116
Video Intelligence Camera Alarms . . . . . 117
Creating a Video Intelligence Camera Alarm . . . . . 118
Editing a Video Intelligence Camera Alarm . . . . . 120
Disabling Video Intelligence Camera Alarm . . . . . 121
Deleting a Video Intelligence Camera Alarm . . . . . 122

## Camera Scheduler

Overview . . . 123
Create a Recording Schedule . . . 123
Enabling/Disabling the Recording Schedule . . . 126
Editing the Recording Schedule . . . 127
Edit the Group Name . . . 127
Edit the Recording Scheduler for a Group . . . 127
Edit the Cameras Assigned to a Schedule Group . . . 128
Remove a Schedule Group . . . 128

## Camera Password Groups

Overview . . . 131
Create a Password Group . . . 131
Delete a Password Group . . . 133

## Basic System Settings

Overview . . . 135
General System Information . . . 135
Hostname . . . 136
Location . . . 137
Current Date and Time . . . 137
Roles . . . 138

## Licensing the NVR

Overview . . . 141
Licensing the NVR . . . 142
Generate a Host ID . . . 142
Apply a Software Licence . . . 143
Software Service Agreement Notifications . . . 143
Edit the SSA Message . . . 143
Edit SSA Contacts . . . 144
Set the SMTP Server Address . . . 145
Send an SSA Test Message . . . 145

## Network Settings


Overview . . . . . 147
Configuring the NVR Network Settings . . . . . 147
General Network Settings . . . . . 149
Domain Name and Domain Name Servers . . . . . 149
Default Gateway . . . . . 150
RTSP Port . . . . . 150
NTP Status and NTP Servers . . . . . 151
LAN Interface Settings . . . . . 152
DHCP Server Settings . . . . . 155
WAN Settings . . . . . 157
WAN IP Address . . . . . 159
HTTP Port . . . . . 159
Secure HTTP Port . . . . . 160
Streaming Configured Port . . . . . 161
Allowed IP Addresses . . . . . 161
Dynamic Bandwidth . . . . . 162
Bandwidth Priority . . . . . 163
Traffic Smoothing Only . . . . . 164
Preserve Framerate . . . . . 165
Preserve Resolution . . . . . 166
Allow Any Throttle Type . . . . . 167


## System Shutdown and Reset Factory Defaults


Overview . . . . . 169
Restart NVR Services . . . . . 169
Stop NVR Services . . . . . 170
Reboot the NVR . . . . . 171
Shutdown the NVR . . . . . 171
Reset Factory Defaults . . . . . 172


## NVR Failover, Configuration Backup, Templates and Updates


Overview . . . . . 177
NVR Failover Mode . . . . . 177
Configure Failover Mode for an NVR . . . . . 179
Disable Failover Mode . . . . . 179
Configuration Backup and Restore . . . . . 180
Create a Configuration Backup File . . . . . 181
Restore an NVR . . . . . 182

Templates . . . . . 184
Save a Configuration Template . . . . . 185
Import a Template File . . . . . 186
Applying Software Updates . . . . . 187
Updating Camera Handler Packs . . . . . 188

## Operational Statistics

Overview . . . . . 189
Recording Performance . . . . . 189
Recording Statistics . . . . . 190
Disk Activity . . . . . 193
Storage Statistics . . . . . 194
Storage Set Statistics . . . . . 194
Storage Device Statistics . . . . . 195
Storage Statistics per Camera . . . . . 196

## Logs

Overview . . . . . 199
Retrieving Logs . . . . . 199
FTP Log Management . . . . . 201
Event Logs . . . . . 202
Camera Connection Errors . . . . . 203
Camera Logs . . . . . 204
Audit Trail . . . . . 206
Viewing Connected Clients . . . . . 207

## Email Alerts

Overview . . . . . 209
Advance Preparation . . . . . 209
Setting Up Email Alerts . . . . . 210
SMTP Server IP Address . . . . . 210
Building the Recipient List . . . . . 211
Enabling and Disabling Email Alerts . . . . . 212
Disabling Email Alerts for a Camera . . . . . 213
Removing an Address from the Recipient List . . . . . 214
Alert Logs . . . . . 215
Clearing the Alert Logs Page . . . . . 216

## Dark Image Detection

Overview . . . 217
Enable Dark Image Detection . . . 218
Enable/Disable Camera Loss Detection . . . 218

## Appendix A: Storage

Overview . . . 221
Storage Concepts . . . 221
iSCSI . . . 221
Fibre Channel . . . 221
Direct Attached Storage . . . 222
Storage Types . . . 222
JBOD . . . 222
RAID . . . 222
Virtual Disks (Logical Unit Numbers) . . . 223
Storage Strategy . . . 224
Understanding Storage Sets . . . 225
Calculating Storage Requirements . . . 226
Overview of AD Fibre RAID Storage (FRS/FES) . . . 227
Second generation American Dynamics iSCSI and Fibre RAID Storage . . . 228
Storage Strategy for FRS/FES RAID Device . . . 228
Recommendations . . . 228
Connecting Additional Storage Devices . . . 228
Connecting NVR to FRS/FES Using Fibre . . . 228
Connecting NVR to FRS/FES Using iSCSI . . . 230

## Appendix B: Web Client Pre-configuration

Overview . . . 237
Prerequisite Software . . . 237
Configuring the Paging File . . . 237
Setting QuickTime Preferences . . . 240
Setting QuickTime Preferences (XP) . . . 241
Setting QuickTime Preferences (Windows 7) . . . 242

## Appendix C: Networking Troubleshooting

Overview . . . 245
Assigning an IP Address to a Client PC . . . 246
Troubleshooting Network Connections . . . 252
Launching the Windows Command Prompt . . . 253
Troubleshooting with the Ipconfig /All Command . . . 255
Troubleshooting with the Ping Command . . . 257
Troubleshooting with the Tracert Command . . . 258

## Appendix D: NVR Troubleshooting

Overview . . . 261
Enabling Remote Desktop . . . 261
Enabling RDP Remote Desktop . . . 261
Enabling VNC Remote Desktop . . . 263
Accessing the Remote Desktop . . . 264
RDP Remote Desktop . . . 264
Logging Out of RDP Remote Desktop . . . 266
VNC Remote Desktop . . . 267
Editing the Network Settings Using Control Center . . . 270
Editing Storage Partitions Using Partitioner . . . 272
Configuring System Partitions on a Previously Configured Device . . . 272
Editing Media Partition Configurations . . . 273
System Disk Recovery . . . 275
VideoEdge NVR . . . 275

## Appendix E: Upgrading your NVR 4.1

Overview . . . 279
Download and Deletion of NVR 4.1 ISO Files . . . 279
NVR 4.1 to NVR 4.2.1 Upgrade . . . 280
Using the 4.1 Upgrade Tool to Launch the YaST Wizard . . . 282
Using the YaST Wizard . . . 284
Completing the Upgrade . . . 288
Changing the Disk Boot Order . . . 291
NVR 4.1 to 4.2.1 Migration Failure Recovery . . . 292

**End User License Agreement (EULA) 295**

**Index 301**

# Overview of the VideoEdge NVR

## NVR Introduction

The VideoEdge Network Video Management System is a scalable enterprise IP video surveillance solution. It is designed as an open platform solution supporting a range of third party hardware, storage, video devices, and clients, allowing users to manage their video surveillance servers and edge devices as a single logical system.

The VideoEdge Network Video Recorder (NVR) manages the IP encoder and camera devices, records the video onto its configured storage devices, and provides clients with secure access to live and recorded video and audio. Users can use a thin-client (NVR Web Interface) and/or the victor rich-client application software to configure the NVR or access the video/audio streams.

## Purpose of the NVR

The NVR is the backbone for an IP-based video security system. The NVR uses TCP/IP communication to access and control the hardware networked to it. The server can be controlled directly by logging into its web interface homepage using a web browser or accessing it via the victor rich-client application software. Worldwide access to the NVR gives it excellent portability - any place where you have a personal computer with internet access to the web, you've got access to your video security system.

An NVR gives you control over all the features of the surveillance and security hardware networked to the NVR. Thus, from your web browser or via victor, you have control over your entire video security system.

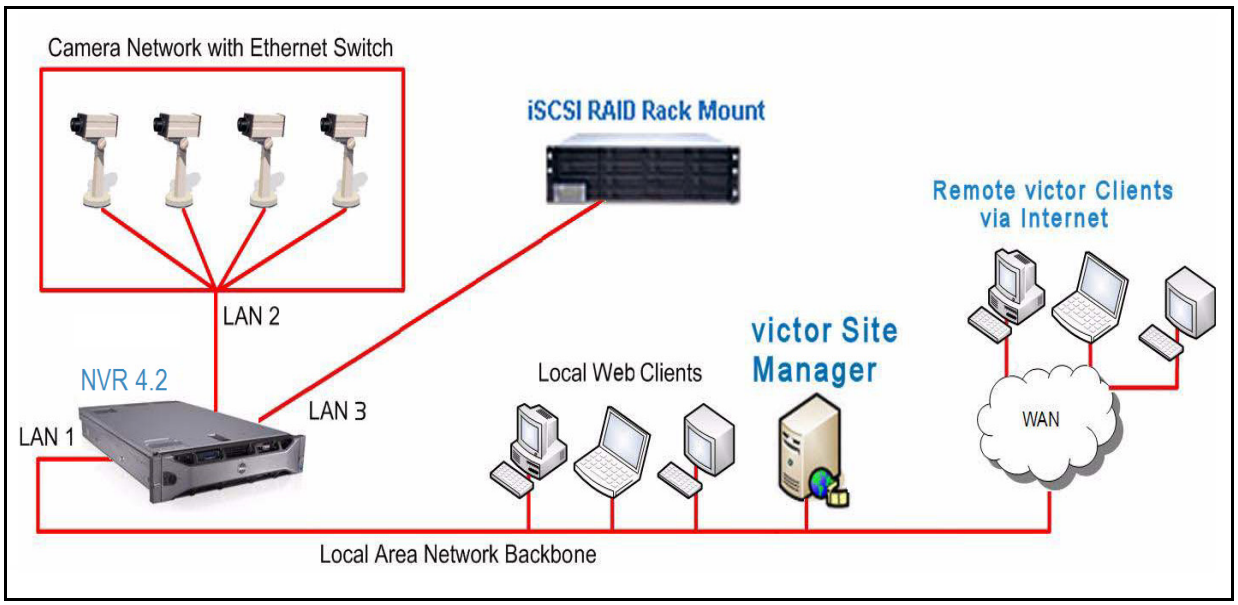
The NVR is available as either a bundled hardware solution or as software-only model that transforms a standard computer hardware system into an advanced and powerful NVR server. The NVR software is a hardware-independent platform.It supports major-brand IP camera and encoder devices, integrates into a TCP/IP networking environment, turning an ordinary PC or server into an Enterprise Network Video Recorder.

## victor Digital Video Management System

The "open" architecture of the victor Digital Video Management System line is designed so that each component can operate independently, and can interact with software applications from other product lines. The victor Digital Video Management System line includes products to address the needs of a wide range of users.

As the architecture is open, it is independent of specific hardware platforms. The NVR does not require an existing operating system as it includes it's own Linux-based operating system that can support a variety of different hardware platforms. Figure 1-1 shows how the NVR fits into the victor Network Video Management System.

**Figure 1-1 VideoEdge Network Video Components**




The **NVR** manages the video camera, storage, and sensor assets for your site. Refer to Getting Started with VideoEdge NVR on page 2 for more information on using the NVR.

You use the **NVR Web Interface** to configure and manage the NVR via a web browser. You can use these web pages to configure the NVR and its storage, cameras, and devices. Typically, the assets connected to the NVR are configured on a local TCP/IP network, isolated from the larger network, and accessible to clients via the NVR and the **victor site manager**. Refer to Using the NVR Interface on page 51 for more information on using the NVR software.

The victor site manager provides a single point of access for users to manage multiple NVRs. The victor site manager utilizes SQL Server's database functionality to provide authentication for VideoEdge Clients, as well as central monitoring and administration of multiple recording platforms over a Wide Area Network (WAN). Refer to the victor Configuration and User Guide for more information on configuring and using the victor site manager software. The **victor clients** are used to monitor and configure one or more NVRs or other devices that are connected to the victor site manager network. The victor client enables a user to login and access multiple NVRs from a single Graphical User Interface (GUI). Refer to the Configuration and User Guide more information on using the victor client software.

# Getting Started with VideoEdge NVR

This manual provides you with the information you need to install, configure and operate the VideoEdge NVR. The main sections of this manual and primary functions of the NVR are outlined below, including references to the relevant sections in the manual to explain how to set up and use the features.

**System Configurations** - provides information on the system configurations of the NVR units. Refer to **System Specifications on page 5**.

**Installation** - provides instructions on how to install the NVR and configure it on the network. Refer to Installing the VideoEdge NVR on page 7.

**NVR Storage** - provides information about the NVR physical storage of video, and instructions on verifying and configuring storage and storage sets. Refer to Configuring Storage on page 59 or Appendix A: Storage on page 221.

**Using the NVR Interface** - provides information on how to access the NVR Configuration Interface via a web browser or via victor unified client and information on how to navigate the interface. Refer to Using the NVR Interface on page 51.

**Camera List** - provides information on how to add IP cameras to the NVR manually or using Auto-Discovery. Refer to **Live Video on page 73**.

**Camera Configuration** - provides information on how to configure cameras as individual cameras or as a batch. Refer to Camera Configuration on page 85.

**Motion Detection** - provides information on how to enable a camera for motion detection and configure motion detection alarms. Refer to Motion Detection on page 103.

**Video Intelligence** - provides information on how to enable a camera for video intelligence and configure video intelligence alarms. Refer to Video Intelligence on page 113.

**Licensing the NVR** - provides information on your current license, how to licence your NVR, how to upgrade your licence and how to configure Software Service Agreement notifications. Refer to Licensing the NVR on page 141.

**Network Settings** - provides information on the current NVR network settings, including LAN, WAN, Dynamic Bandwidth and DHCP Server settings. It also provides information on how to edit the current settings. Refer to Network Settings on page 147.

**Failover, Configuration Backup, Templates and Updates** - provides information on how to configure the NVR as a Failover server, create backup and template files and how to configure the NVR using configurations saved in backup and template files. This chapter also describes how to install system updates and patches and how to update the camera handler packs. Refer to NVR Failover, Configuration Backup, Templates and Updates on page 177.

# System Specifications

## Overview

The VideoEdge NVR 4.2.1 release is available as a hardware and software bundle or as stand alone software.

The bundled hardware and software is delivered with the software installed on the provided hardware.

The software only model is distributed on a disk or USB drive. The NVR software can be installed on any hardware platform that meets the recommended system specifications.

### System Specifications

The hardware platforms that have been tested and qualified as supported systems for hosting the NVR software are detailed in this section. The amount of video storage needed depends on site requirements, such as the video retention period, the number of cameras, and the settings for the resolution, frame rate, codec and quality.

### System Specifications for Bundled Packages

The below hardware platforms are available, as tested and qualified systems, as part of the bundled NVR hardware and software package.

### Table 2-1 Hardware and Software Bundle System Specification

| | |
|---|---|
| **Processor** | Single Intel E2620. |
| **Memory** | 8GB (4 x 2GB modules). |
| **System Drive** | Minimum 500GB Hard-Drive |
| **Video Storage** | Minimum 500GB Hard-Drive. |
| **RAID Controller** | PERC H710 Integrated RAID Controller |
| **Network Interface Cards** | Minimum 2 x 1G NICs |
| **Keyboard & Mouse** | Required for installation and setup only. |
| **Monitor** | Required for installation and setup only. |
| **Operating System** | None (OS will be installed with the VideoEdge Software) |

## Recommended System Specifications for Software Only

The following hardware platforms have been tested and qualified as supported systems for hosting the NVR software.

### Table 2-2 Recommended System Specification

| | |
|---|---|
| **Processor** | Single Intel E2620. |
| **Memory** | 8GB (4 x 2GB modules). |
| **System Drive** | Minimum 500GB Hard-Drive |
| **Video Storage** | Minimum 500GB Hard-Drive. |
| **RAID Controller** | PERC H710 Integrated RAID Controller |
| **Network Interface Cards** | Minimum 2 x 1G NICs |
| **Keyboard & Mouse** | Required for installation and setup only. |
| **Monitor** | Required for installation and setup only. |
| **Operating System** | None (OS will be installed with the VideoEdge Software) |

# Installing the VideoEdge NVR

## Overview

This chapter describes the installation and configuration process for the NVR.The NVR is supplied as either a hardware and software bundle or as a software only bundle.

### NVR Hardware and Software Bundle

When the NVR is supplied as a pre-configured hardware and software bundle the basic system settings including time and region are already applied. The system will also have default partitioning already carried out including the required system partitions and some media partitions. If the configured media partitions are not suitable these can be edited as required after installation, for further information refer to Editing Storage Partitions Using Partitioner on page 272.

The NVR is supplied with its NIC eth0 enabled, it's set to resolve a DHCP IP address or will be assigned a default static IP address of 10.10.10.10 if DHCP is not available. All other NICs of the NVR will be supplied disabled. The network settings for the NVR are configured using the Setup Wizard.

### NVR Software Only Bundle

When the NVR is supplied as a software only bundle it requires full installation onto your hardware. You should ensure your hardware matches the minimum operation requirements, refer to System Specifications on page 5.

## Installing the NVR Hardware and Software Bundle

This section details the installation and configuration process for an NVR hardware and software bundle.

The installation and configuration process consists of:

**1** Initial boot up of the NVR

**2** Setting up NVR OS User Accounts

**3** Logging into the NVR desktop

**4** Configuring the NVR using the Setup Wizard.

# Initial Boot Up of the NVR

## Procedure 3-1
## Powering up the NVR for the First Time

| Step | Action |
|---|---|
| 1 | Power up the NVR.<br>A series of boot messages appear and the system is loaded to the Licence Agreement. |
| 2 | When the licence agreement is displayed, select **Yes, I Agree to the Licence Agreement**. |
| 3 | Click **Next**.<br>Set the Password for the Root User account page displays. The next stage of installation process is to create user accounts. |

**- End -**

## Procedure 3-2
## Setting Up NVR OS User Accounts

| Step | Action |
|---|---|
| 1 | In the Password field in the Root User account page of the Installer, enter a password for the root user account. |

### Caution

It is extremely important that you will remember this password. If necessary you should write this password down and store it securely.

| | |
|---|---|
| 2 | Re-enter the password in the **Confirm Password** field. |
| 3 | Click **Next**. |
| 4 | If the system does not recognize the password as secure, a message opens. Click **Yes** to confirm the use of the weak password and continue, or click **No** to change the password. A secure password should contain both upper and lower case letters, numbers and special characters.<br>**Note**<br>If the passwords entered into the Password and Confirm Password fields do not match, a message opens. Re-enter the passwords to continue. |
| 5 | Create an operator user account:<br>**a** Enter the **User's Full Name**. |

**b** Enter a **Username**.

**Note**

A name is suggested depending on the User's Full Name.

**c** Enter a **Password**.

**d** Re-enter the password in the **Confirm Password** field.

**e** Click **Next**.

**Note**

1 If the system does not recognize the password as secure, a message opens. Click **Yes** to confirm the use of the weak password and continue, or click **No** to change the password. A secure password should contain both upper and lower case letters, numbers and special characters.

2 If the passwords entered into the **Password** and **Confirm Password** fields do not match, a message opens. Re-enter the passwords to continue.

Or

If you do not want to create an operator user account:

**a** Leave the **User's Full Name**, **Username**, **Password** and **Confirm Password** fields empty.

**b** Click **Next**.

A message opens stating 'Empty User Login' and asking for confirmation to 'Leave it empty'.

**c** Click **Yes**.

**Note**

It is highly recommended to setup an operator account when prompted in addition to the root user account. The root user account should be used for troubleshooting and system OS setup only.

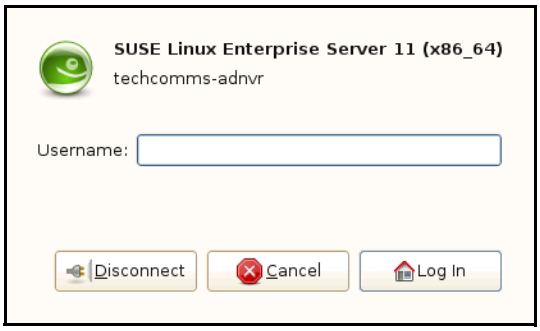
**6** To continue with the installation and configuration process you need to log in to the NVR desktop.

**- End -**

## Logging into the NVR Desktop

After setting the root password and creation of the administration user you are required to login to the NVR desktop to continue the installation and configuration process.

**Figure 3-1 NVR Login Screen**




### Procedure 3-3
### Logging into the NVR Desktop

| Step | Action |
|---|---|
| 1 | When the system boots to the NVR login screen. Enter the Administrator **Username**. |
| 2 | Click **Log In**. |
| 3 | Enter the Administrator **Password**. |
| 4 | Click **Log In**.<br>On successful login, the NVR desktop is displayed. |

**- End -**

To complete the installation and configuration process you need to complete the Setup Wizard, continue to VideoEdge Setup Wizard on page 25.

# Installing the NVR Software Only Bundle

This section details the installation and configuration process for an NVR software only package.

Before installation you must ensure that the system drive is connected to the SATA 0 location on the motherboard.

The installation and configuration process consists of:

1. (Optional) Verifying the BIOS Configuration
2. Booting the system using the NVR software disk
3. Using the NVR Wizard to:
   - **a** Configure system information settings
   - **b** Configure disk partitions

c Verify the boot loader location

d Complete basic installation

4 A system reboot after basic installation

5 Setting up NVR OS user accounts

6 Logging into the NVR desktop

7 Configuring the NVR using the Setup Wizard

## Verify the BIOS Configuration

If required you may need to verify the system BIOS settings before installing the NVR software.

### Procedure 3-4
### Verify BIOS Configuration

| Step | Action |
|---|---|
| 1 | Power on the system. |
| 2 | While the system is booting up, enter the BIOS menu by pressing the appropriate key. Usually, the system will inform you of the appropriate key during bootup, but refer to your user manual if necessary. |
| 3 | Confirm that all of the installed devices (e.g. hard drives and CD/DVD drives) are recognized. |
| 4 | Do not adjust the time or date in BIOS. You will set the date and time on the Server's web-based interface. |
| 5 | Confirm that the hyper-threading is enabled if it is available. |
| 6 | Confirm that the **1st Boot Device** is CD/DVD or Alternative Hard Disk (USB) and **2nd Boot Device** is the hard drive. |
| 7 | Select **Save and Exit Setup** to reboot the system with the above settings. |

**- End -**

## Boot your Computer/Server Using the NVR Software CD or USB

To initialize the installation of the NVR, the system must boot from the software CD or USB.

### Procedure 3-5
### Boot your Computer/Server Using the NVR Software CD or USB

| Step | Action |
|---|---|
| 1 | Insert the NVR software CD into the optical drive or insert the NVR Installation USB drive into one of the available USB ports and restart your computer/server. |

2 The NVR boots from the CD or USB drive and the installation options menu opens.

**Note**

If the NVR does not boot from the disk, please review your computer/server BIOS option to boot from optical drive or USB. Please check your computer/server function key to enter boot order (Procedure 3-4 Verify BIOS Configuration on page 11).

3 From the installations option menu select **NVR Live Installer**.

**Note**

After approximately 20 seconds the installation will automatically start in this mode.

A Loading Linux Kernel pop up displays followed by a series of boot messages. This process may take several minutes.

When the system has finished the initial software installation and restart, the NVR desktop opens.

**Note**

The VideoEdge NVR software will install the minimum required Linux Operating System to run the NVR (The NVR software is installed as an appliance).

4 Double-click the **NVR Installer** icon to launch the installation tool.

A Terminal pop-up window displays a loading sequence, and the Live Installer opens.

5 The next stage of the installation process is to configure the NVR's system information settings.

**- End -**

## Configure the NVR's System Information Settings

Using the Installer to configure the system information settings, including the NVR language, keyboard layout, date and time.

### Procedure 3-6
### Configuring the NVR System Information Settings

| Step | Action |
|---|---|
| 1 | In the Welcome page of the Installer, select the required **Language** from the dropdown. |
| 2 | Select the **Keyboard Layout** from the dropdown. |
| 3 | After reading the licence agreement, select the **I Agree to the Licence Terms** checkbox. |
| 4 | Click **Next**.<br>The Clock and Time Zone page displays. |
| 5 | Select the **Region** from the dropdown. |

6 Select the **Time Zone** from the dropdown.

The date and time for the selected time zone is displayed.

**Note**

1 If the time and date settings are not correct you can manually update the settings by clicking the **Change...** button and manually entering the current date and time, or synchronize with the NTP server.

2 For reliable time based playback both the NVR and Client PC need to be configured as clients of the same NTP server.

7 (Optional) Select the **Hardware Clock Set To UTC** checkbox.

**Note**

You should only select this checkbox if the system's hardware clock is set to UTC.

8 Click **Next**.

The Suggested Partitioning page displays.

**- End -**

## Configure Storage Partitions

After the system information settings have been configured for the NVR, you can set up the required storage partitions.

The NVR's storage consists of system and media partitions. System partitions are where the operating system and VideoEdge software resides and system files such as swap and var are stored. The System partitions consists of 3 parts:

1 The root partition (**/**). This is where the operating system, VideoEdge software and executables are stored.

2 The var partition (**/var**). This is where configuration and other variable 'non-video' files are stored.

3 The swap partition (**/swap**). This is the location of the operating system swap file.

Media partitions are where audio and video from the associated cameras will be stored.

**Note**

On the first media drive of the NVR you must create two media partitions. The first partition created on this drive must be 100GB with the mount point **/var/opt/americandynamics/venvr/clipexport**. The size of the second partition must be the remainder of the media drive. You can enter a mount point name as required, for example, **/data1**. It is recommended that the remaining media drives on the NVR are configured with 1 partition and formatted in the XFS file system type.

If this is the first time the NVR 4.2.1 software has been installed on the system, the default system partitions will already be configured. The system partitions are needed for regular operation of the operating system and NVR application. The default system partitions defined are in Table 3-1 below. Each partition size in the table is the **required** value. If it is not the first time the NVR 4.2.1 software has been installed in the system, partitions need to be deleted and recreated, refer to

Configuring System Partitions on a Previously Configured Device on page 272.

### Table 3-1 Default Partitions Required for NVR

| Size (GB) | Type | FS Type | Mount Point |
|---|---|---|---|
| 16 | Linux swap | Swap | swap |
| 476 | Linux native | XFS | /var |
| 8 | Linux native | Ext3 | / |

## Procedure 3-7
## Configuring Media Partitions on the First Media Drive on the NVR

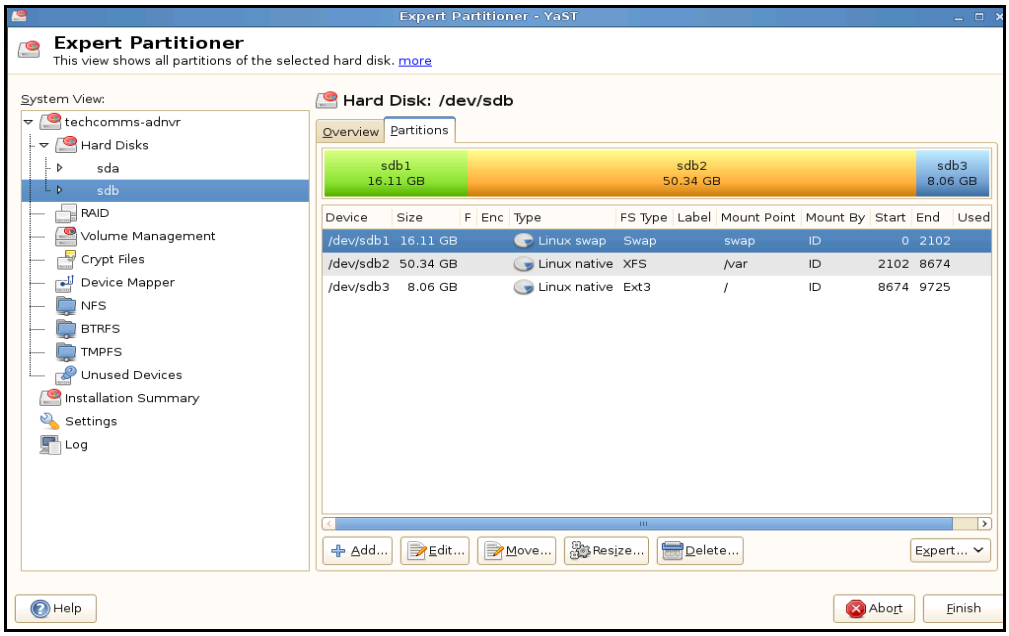
| Step | Action |
|---|---|

**1** In the Suggested Partioning page of the wizard, click **Create Partition Setup**.

**2** Select **Custom Partitioning (for experts)**.

**3** The Expert Partitioner page opens.

### Figure 3-2 Expert Partitioner Page




**4** Select the first media drive from the system view tree.

**Note**

Disks may have existing partitions. If this is the case they should be removed before reconfiguring a storage device by adding partitions. Removing any storage partitions will destroy any existing data.

**5** Click **Add.**

**6** Select **Primary Partition**.

**7** Select **Custom Size** and enter **100GB** to allocate to the partition.

8 Select **Next**

9 Click the **Format partition** option button.

10 Select **XFS** from the **File System** dropdown.

11 Enter the **Mount Point** for the media partition. Enter **/var/opt/americandynamics/venvr/clipexport**

12 Select the **Fstab Options...** button.

13 Enter **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

14 Click **OK**.

15 Click **Add.**

16 Select **Primary Partition**.

17 Select the **Maximum Size** option to use the remaining disk space.

18 Select **Next**

19 Click the **Format partition** option button.

20 Select **XFS** from the **File System** dropdown.

21 Enter the **Mount Point** for the media partition, for example, **/data1**.

22 Select the **Fstab Options...** button.

23 Enter **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

24 Click **OK**.

**- End -**

## Procedure 3-8
## Configuring Media Partitions on the Remaining Media Drives on the NVR

| Step | Action |
|---|---|

1 In the Suggested Partioning page of the wizard, click **Create Partition Setup**.

2 Select **Custom Partitioning (for experts)**.

The Expert Partitioner page opens.

3 To create storage space for media data, you are required to create media storage partitions. Select the disk on which you want to create the media partition from the system

view tree. This can be either the hard disk on the NVR itself or on separate RAID or FRS storage devices.

**Note**

Disks may have existing partitions. If this is the case they should be removed before reconfiguring a storage device by adding partitions. Removing any storage partitions will destroy any existing data.

4 Click **Add.**

5 Select either **Primary Partition** or **Extended Partition**.

**Note**

A **Primary Partition** contains one file system. Up to four primary partitions can be created on a single hard drive.

An **Extended Partition** is a primary partition that has been divided up into logical partitions as a means of creating more partitions than the four that would otherwise be possible. Only one primary partition can be used as an extended partition, and it can be created from any of the primary partitions. The logical partitions do not need to fill the entire extended partition.

6 Enter the required partition size. You can select the Maximum Size option to use the remaining disk space, or select Custom Size and enter the amount of disk space (GB) you want to allocate to the partition.

Or

Choose an allocated region on the disk for the partition by entering a Start Cylinder and End Cylinder.

**Note**

In order to use a disk partition for storage it must meet the minimum storage capacity requirements, 10GB.

7 Select **Next**

8 If you are creating an extended partition, go to Step 16, otherwise continue to Step 10.

9 Click the **Format partition** option button.

10 Select **XFS** from the **File System** dropdown.

11 Enter the **Mount Point** for the media partition, for example, **/data/media1**.

12 Select the **Fstab Options...** button.

13 Enter **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

14 Click **OK**.

15 Click **Finish**.

16 Repeat Steps 3 to 15 to create additional media storage partitions.

17 Once the required number of media partitions are created click **Accept**.

A summary of the partitions to be created are displayed. If you want to edit any of the partitions click **Edit Partition Setup** and make the changes as required.

18 Click **Next.**

A summary of the partition layout to be created is displayed.

19 Click **Install.**

The Live Installation Settings page is displayed.

20 Continue to Verify the Boot Loader location.

**- End -**

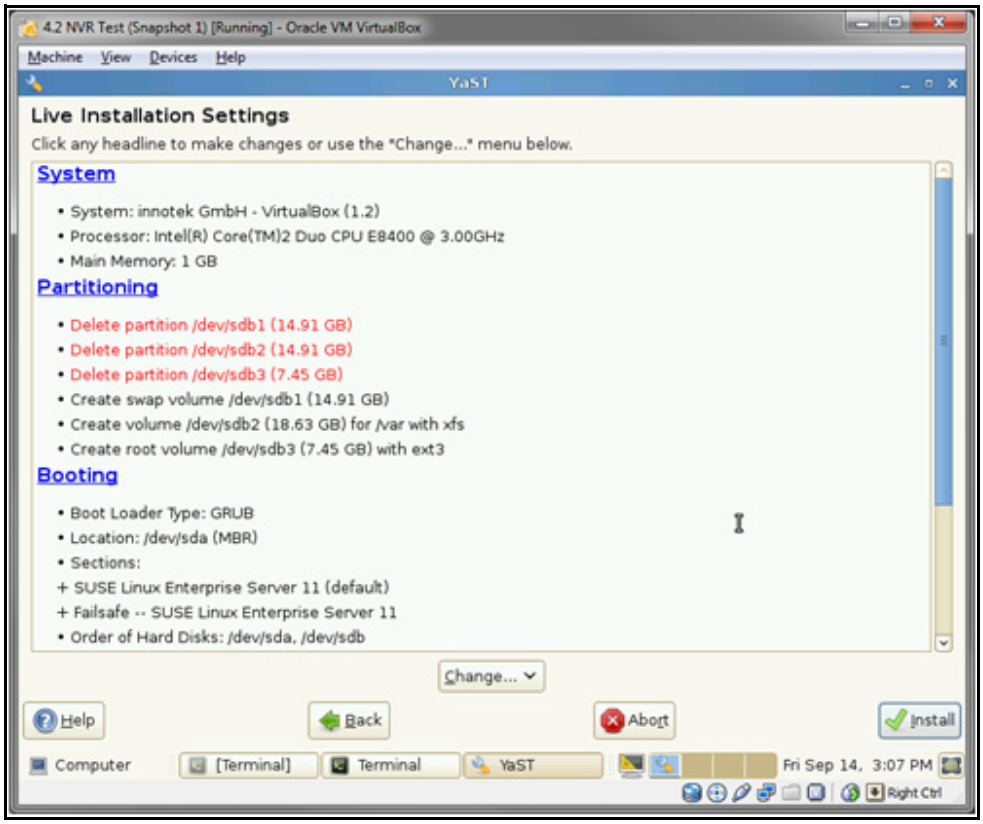
## Verify the Boot Loader location

The boot loader must be on the same disk where the operating system software will be installed. If the boot loader is not on the same disk the system software is located system boot problems may occur.

Before confirming installation you can compare the location of the boot loader and the location chosen for system installation and partitioning.

In Figure 3-3 Live Installation Settings below the installer has chosen to use the disk **/dev/sdb** for the partitioning proposal but the disk on which to install the boot loader is **/dev/sda**.

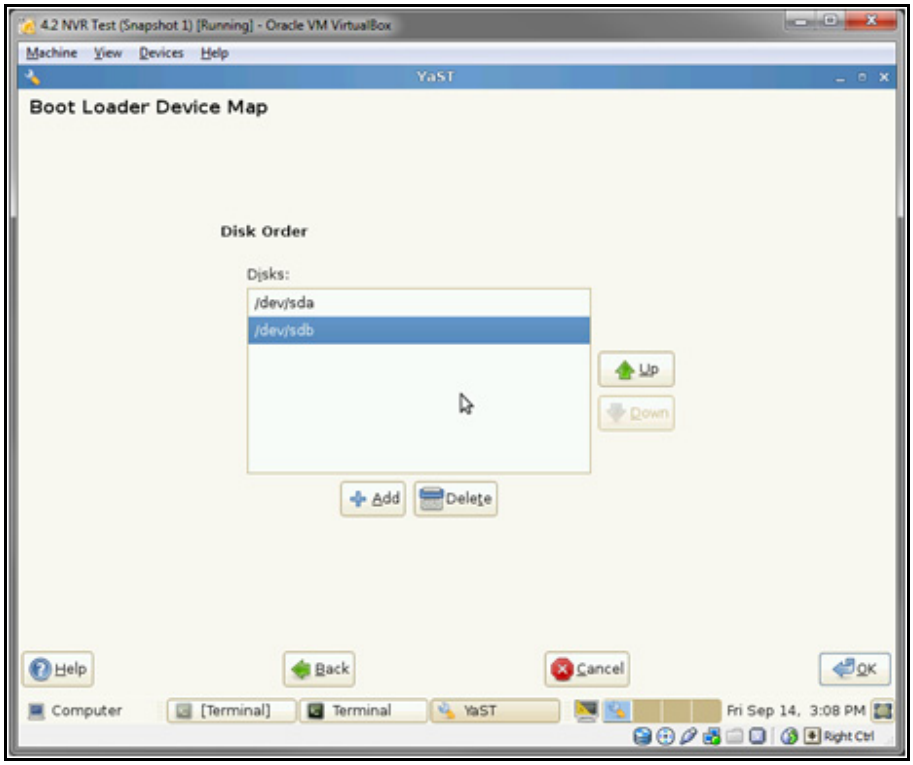
**Figure 3-3 Live Installation Settings**


4.2 NVR Test (Snapshot 1) [Running] - Oracle VM VirtualBox
Machine View Devices Help
YaST
Live Installation Settings
Click any headline to make changes or use the "Change..." menu below.
System
• System: innotek GmbH - VirtualBox (1.2)
• Processor: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz
• Main Memory: 1 GB
Partitioning
• Delete partition /dev/sdb1 (14.91 GB)
• Delete partition /dev/sdb2 (14.91 GB)
• Delete partition /dev/sdb3 (7.45 GB)
• Create swap volume /dev/sdb1 (14.91 GB)
• Create volume /dev/sdb2 (18.63 GB) for /var with xfs
• Create root volume /dev/sdb3 (7.45 GB) with ext3
Booting
• Boot Loader Type: GRUB
• Location: /dev/sda (MBR)
• Sections:
+ SUSE Linux Enterprise Server 11 (default)
+ Failsafe -- SUSE Linux Enterprise Server 11
• Order of Hard Disks: /dev/sda, /dev/sdb
Change...
Help
Back
Abort
Install
Computer
[Terminal]
Terminal
YaST
Fri Sep 14, 3:07 PM
Right Ctrl

## Procedure 3-9
## Verifying the Boot Loader Location

| Step | Action |
|---|---|
| 1 | Check the boot loader location on the Live Installation Settings page.<br><br>If the location for the boot loader is on the same disk as where the software operating system will be installed, click **Install** and continue to Procedure 3-10 Rebooting the NVR After Basic Installation.<br><br>**Note**<br>Installation may take up to ten minutes depending on computer/server hardware.<br><br>If the location of the boot loader is on a different disk you need to change the boot loader location. Continue to Step 2. |
| 2 | In the Live Installation Settings page select the **Booting** hyperlink. |
| 3 | Select the **Boot Loader Installation** tab. |
| 4 | Select **Boot Loader Installation Details.**<br><br>The boot loader Device map page opens as shown in Figure 3-4 below. |

**Figure 3-4 Boot Loader Device Map**



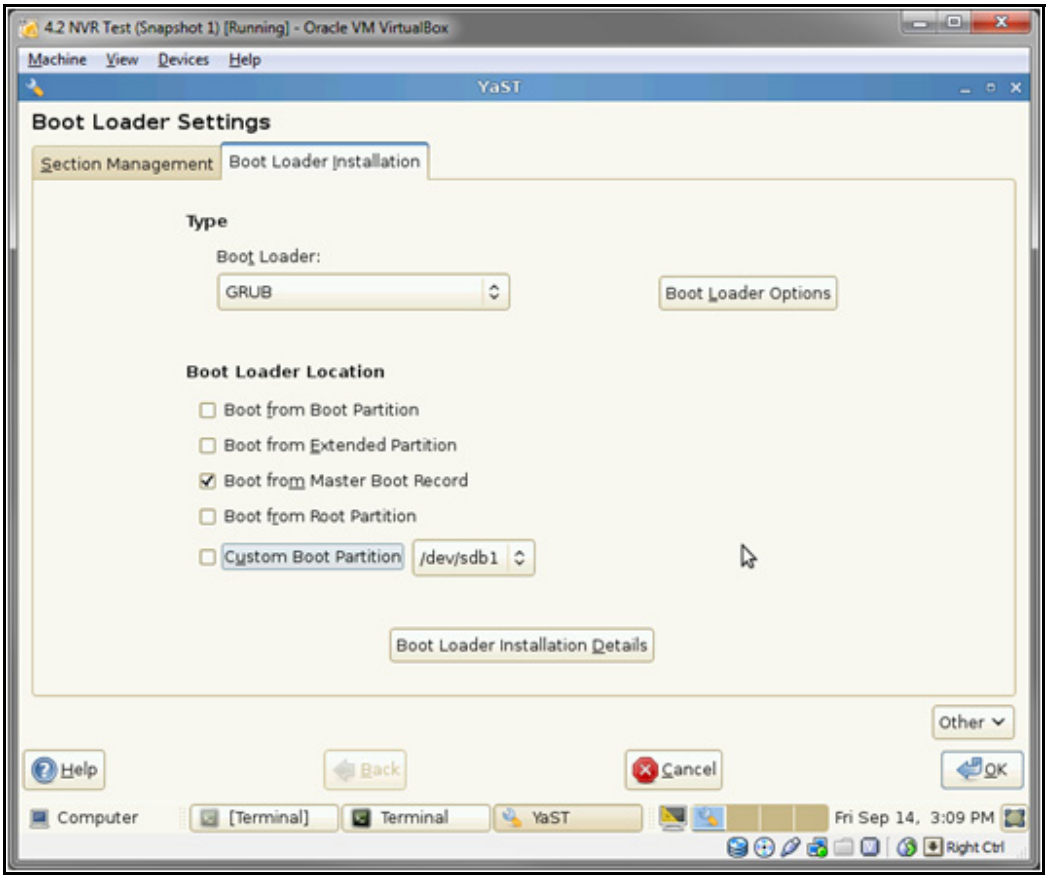

5 Select the disk that has the operating system installed from the Disk Order list. In the example shown this is **/dev/sdb**.

6 Click **Up** to move the selected disk to a higher position in the Disk Order list. Continue to click **Up** until the operating system disk is at the top of the list.

7 Click **OK**.

The Boot Loader settings page is displayed as shown in Figure 3-5 below.

**Figure 3-5 Boot Loader Settings**



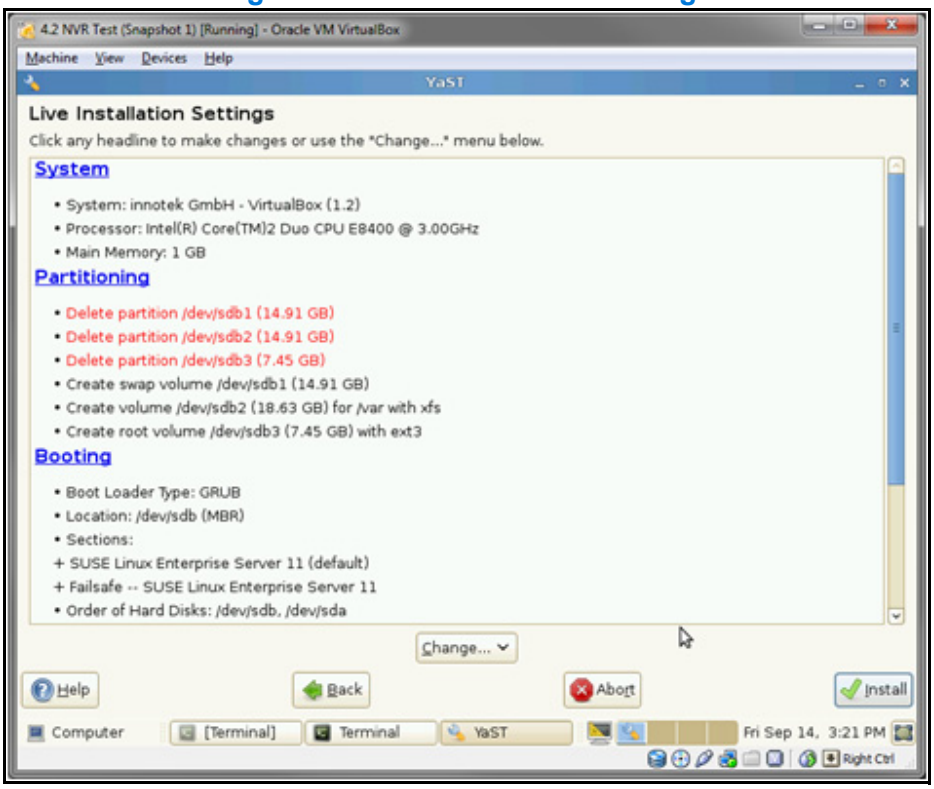

**8** Ensure the **Custom Boot Partition** checkbox is unchecked.

**9** Click **OK** to return to the Live Installation Settings page.

**10** Confirm on the Live Installation Settings page that the GRUB boot loader and the operating system are now configured on the same drive.

In the example shown in Figure 3-6 below the operating system is set to be installed on partitions **/dev/sbd1**, **/dev/sdb2/** and **/dev/sdb3**. The boot loader will be installed on to the Master Boot Record (MBR) of **/dev/sdb**.

Figure 3-6 Live Installation Settings


4.2 NVR Test (Snapshot 1) [Running] - Oracle VM VirtualBox
Machine View Devices Help
YaST
Live Installation Settings
Click any headline to make changes or use the "Change..." menu below.
System
• System: innotek GmbH - VirtualBox (1.2)
• Processor: Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz
• Main Memory: 1 GB
Partitioning
• Delete partition /dev/sdb1 (14.91 GB)
• Delete partition /dev/sdb2 (14.91 GB)
• Delete partition /dev/sdb3 (7.45 GB)
• Create swap volume /dev/sdb1 (14.91 GB)
• Create volume /dev/sdb2 (18.63 GB) for /var with xfs
• Create root volume /dev/sdb3 (7.45 GB) with ext3
Booting
• Boot Loader Type: GRUB
• Location: /dev/sdb (MBR)
• Sections:
+ SUSE Linux Enterprise Server 11 (default)
+ Failsafe -- SUSE Linux Enterprise Server 11
• Order of Hard Disks: /dev/sdb, /dev/sda
Change...
Help
Back
Abort
Install
Computer
[Terminal]
Terminal
YaST
Fri Sep 14, 3:21 PM
Right Ctrl

**11** Click **Install**.

**Note**

Installation may take up to ten minutes depending on computer/server hardware.

**12** Continue to System Reboot After Basic Installation.

**- End -**

## System Reboot After Basic Installation

After basic installation is complete the NVR must be restarted to progress to the next stage of the installation process.

**Note**

If you forget to remove the software CD or USB from the computer/server you will be given the option to select '**Boot from Hard Disk**'.

### Procedure 3-10
### Rebooting the NVR After Basic Installation

| Step | Action |
|---|---|

**1** After basic installation is complete a Finished Basic Installation dialog appears. Click **OK**.

The Live Installer closes and the Terminal Window opens.

2 Use the keyboard to enter **Y** followed by the **[Enter]**, in the Terminal Window.

3 Ensure the BIOS splash screen is displayed. Remove the disk or detach the USB drive.

The NVR reboots and the installation options menu opens.

**Caution**

It is not recommended to remove the disk or USB before the BIOS splash screen is displayed.

4 (Optional) If you do not remove the disk/USB, use the keyboard to select **Boot from Hard Disk** and press the **[Enter]**.

5 After the system has booted the licence agreement is displayed, select **Yes, I Agree to the Licence Agreement** to continue with the VideoEdge software installation.

6 Click **Next**.

The Password for the Root User account page displays. The next stage of installation process is to create user accounts.

**- End -**

## Set Up NVR OS User Accounts

The next stage of the installation and configuration process is to set a password for the root user account. You also must create an operator user account and password. These accounts will be used for logging into the NVR operating system to access the NVR desktop.

**Note**

It is highly recommended to setup an operator account when prompted in addition to the root user account. The root user account should be used for troubleshooting and system OS setup only.

### Procedure 3-11
### Setting Up NVR OS User Accounts

| Step | Action |
|---|---|

1 In the Password for the Root User account page of the Installer, enter a password for the root user.

**Caution**

It is extremely important that you will remember this password. If necessary you should write this password down and store it securely.

2 Re-enter the password in the **Confirm Password** field.

3 Click **Next**.

**4** If the system does not recognize the password as secure, a message opens. Click **Yes** to confirm the use of the weak password and continue, or click **No** to change the password. A secure password should contain both upper and lower case letters, numbers and special characters.

**Note**

If the passwords entered into the Password and Confirm Password fields do not match, a message opens. Re-enter the passwords to continue.

**5** Create an operator user account:

**a** Enter the **User's Full Name**.

**b** Enter a **Username**.

**Note**

A name is suggested depending on the User's Full Name.

**c** Enter a **Password**.

**d** Re-enter the password in the **Confirm Password** field.

**e** Click **Next**.

**Note**

1 If the system does not recognize the password as secure, a message opens. Click **Yes** to use the password and continue, or click **No** to change the password. A secure password should contain both upper and lower case letters, numbers and special characters.

2 If the passwords entered into the **Password** and **Confirm Password** fields do not match, a message opens. Re-enter the passwords to continue.

Or

If you do not want to create an operator user account:

**a** Leave the **User's Full Name**, **Username**, **Password** and **Confirm Password** fields empty.

**b** Click **Next**.

A message opens stating 'Empty User Login' and asking for confirmation to 'Leave it empty'.

**c** Click **Yes**.

**Note**

It is highly recommended to setup an operator account when prompted in addition to the root user account. The root user account should be used for troubleshooting and system OS setup only.

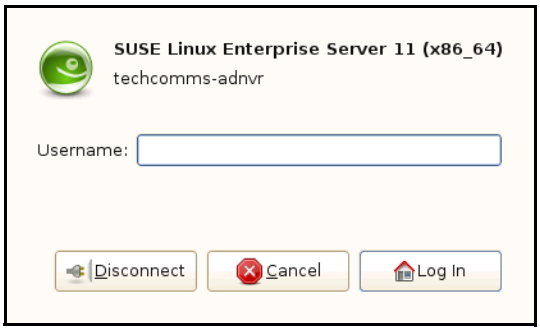
**6** To continue with the installation and configuration process you need to log in to the NVR desktop.

**- End -**

## Log into the NVR Desktop

After setting up user accounts, to continue the installation and configuration process you need to log into the NVR desktop.

**Figure 3-7 NVR Login Screen**




### Procedure 3-12
### Logging into the NVR Desktop

| Step | Action |
|---|---|
| 1 | When the system boots to the NVR login screen. Enter your operator **Username**. |
| 2 | Click **Log In**. |
| 3 | Enter your **Password**. |
| 4 | Click **Log In**. |
| | On successful login, the NVR desktop is displayed. |

**- End -**

## VideoEdge Setup Wizard

Once the NVR has been installed you need to configure the NVR settings via the Setup Wizard. This can be accessed using the **VideoEdge Administrator** icon on the NVR desktop or via a remote client. On the first time accessing the NVR user interface after installation you will be automatically be directed to the Setup Wizard.

**Note**

If you exit the Setup Wizard prior to completing all the steps, the wizard will save your progress and automatically return to the last page viewed of the Setup Wizard.

The Welcome page is the first page of the Setup Wizard. The purpose of the wizard is to aid you in the final stages of the NVR's installation and configuration. On completion your NVR will be operational.

The Setup Wizard provides the option to configure the following:

1 **Preparation** -

- **a** Application of a permanent license, generation of a Host ID, application of a template file (this is pre-defined settings for the NVR).
- **b** Enabling the NVR to act as a Failover Server.

2 **System** -

- **a** Configure the general system information including NVR hostname, location, current date/time.
- **b** Change the passwords for the two user roles of the NVR.

3 **Network** -

- **a** Edit the general network settings including domain name, domain name servers, default gateway, RTSP port, NTP status and NTP servers.
- **b** Edit the LAN settings for each NIC including IP address allocation, LAN IP address, subnet mask and IP broadcast, the MAC address for each NIC can also be viewed.
- **c** Edit the WAN settings including the WAN IP address, HTTP port, secure HTTP port, streaming configured port.
- **d** Edit the Dynamic Bandwidth settings including Bandwidth Priority, Traffic Smoothing, WAN bitrate cap and LAN bitrate cap and Transcode Limit.
- **e** Edit the DHCP settings for each NIC including, DHCP status, IP address start range, IP address end range, subnet and netmask.

4 **Cameras** -

- **f** Add cameras using Discovery.
- **g** Add cameras manually.
- **h** Configure camera alarms.

5 **Storage** -

- **a** Assign custom percentage of storage as the Vault Media Quota. This is the percentage of media storage that is allocated to protected media.
- **b** Enable advanced storage configuration; this allows you to configure custom storage sets, assign cameras to specific storage sets and specify maximum retention period per camera.

6 **Email Alerts** -

**a** Assign the SMTP server IP address.

**b** Add a recipient email address with selectable alert categories including system alerts, storage alerts, motion detection alerts analytics alerts, camera malfunction, reboot notification, camera(s) not recording, no storage active on unit, failed to read storage config and failover event.

**c** Enable and test alert categories including system alerts, storage alerts, motion detection alerts, analytics alerts, camera malfunction, reboot notification, camera(s) not recording, no storage active on unit, failed to read storage config and failover event.

**7** **Summary** -

**a** Configured settings can be saved to a template file, settings to be saved can be selected using check boxes, they include camera settings, storage settings, user information, network settings, email settings and failover settings.

**b** Setup is completed by selecting Finish.

## Accessing the Setup Wizard

Accessing the NVR Web Interface for the first time will initialize the Setup Wizard. You can use the VideoEdge Administrator icon located on the NVR desktop or login via a remote client.

### Caution

The VideoEdge Administrator icon has been added for convenience. Firefox is not a supported browser for use with the NVR Web Interface. Apart from this stage of installation and configuration Internet Explorer must be used as the browser to access the NVR Web Interface.

### Procedure 3-13
### Opening the NVR Setup Wizard

| Step | Action |
|---|---|

**1** Login to the NVR configuration interface. To login double-click the **VideoEdge Administrator** icon on the SUSE desktop.

OR

Open a web browser from a remote client PC and enter the IP address **10.10.10.10**. This is the default IP address.

The browser opens and automatically connects to the Setup Wizard (Setup Wizard displays after installation when the Web Interface is accessed until the wizard has been completed).

**Figure 3-8 VideoEdge Administrator Icon**

**2** You will be prompted to enter a Username and Password. Enter the following credentials:

Username: **admin**

Password: **VIDEO!edge23**

3 Click **OK**.

The wizard's Welcome page opens.

**- End -**

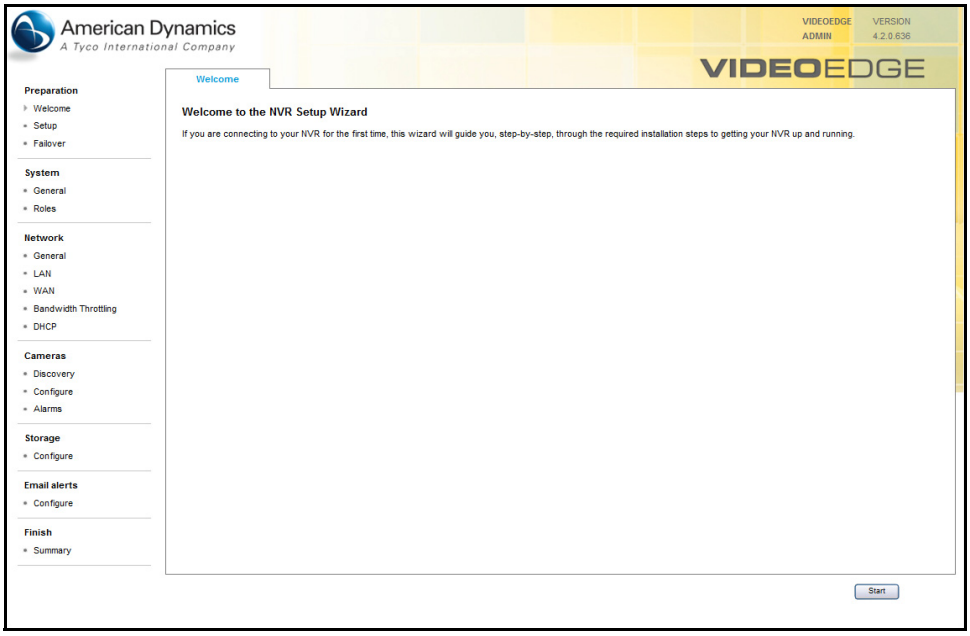
# Preparation

This section describes the preparation stage of the Setup Wizard including the Welcome, Setup and Failover pages.

## Welcome Page

The Welcome page is the first page of the Setup Wizard, to advance to the next page click **Start**.

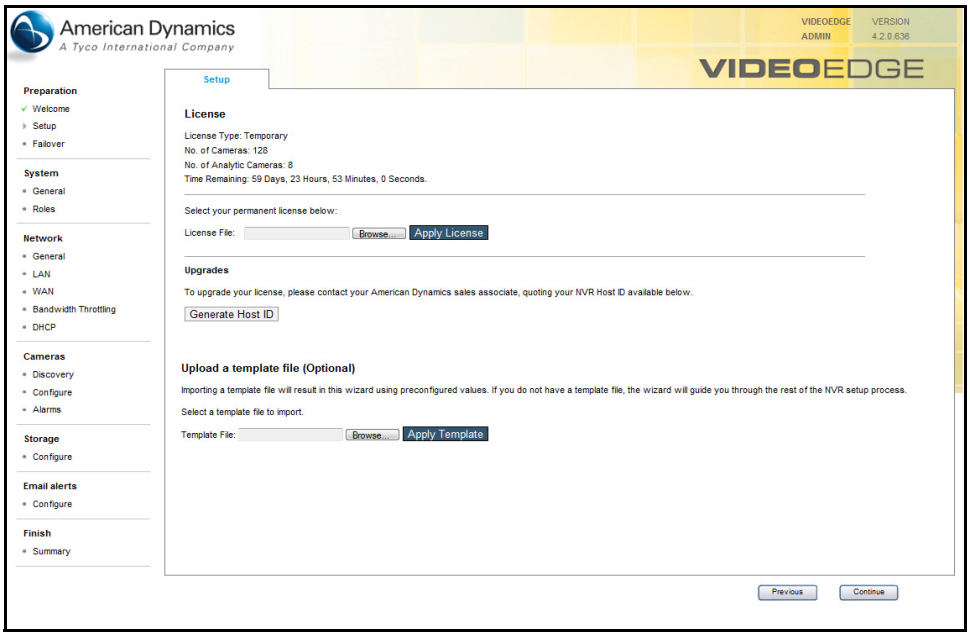
**Figure 3-9 Welcome Page**




## Setup Page

The Setup page provides an interface to apply a licence or generate a host ID. there also is the option to apply template settings. The host ID is required for upgrade and new installations.

**Figure 3-10 Setup Page**




## Procedure 3-14
## Configuring the Setup Page

| Step | Action |
|---|---|

**1** Apply your saved licence file:

- **a** Click **Browse** in the License section. For convenience there is an icon on the desktop with direct access to the American Dynamics.net web site to register your license. In most instances the license will be emailed to you in less than one minute.
- **b** Locate your permanent license file and click **Open**.
- **c** Select **Apply Permanent License**.

Or

Request a licence by generating a Host ID

- **a** Click **Generate Host ID**.

**Note**

Your NVR host ID should be quoted to American Dynamics if you wish to apply for your license. For more information refer to Procedure 14-1 Generate a Host ID on page 142.

Or

To utilize the 60 day trial continue to the next step.

**2** (Optional) Apply a Template file.

- **a** To import a template file, click **Browse** in the Upload a Template file section
- **b** Locate the template file and click **Open**.

c Click **Apply Template**.

**Note**

Using a template file allows you to apply pre-configured values to the NVR, this is very useful if you want to set up more than one NVR with the same configuration. For further information refer to Procedure 17-6 Importing a Template File on page 186.

3 Click **Continue** to advance to the next page.

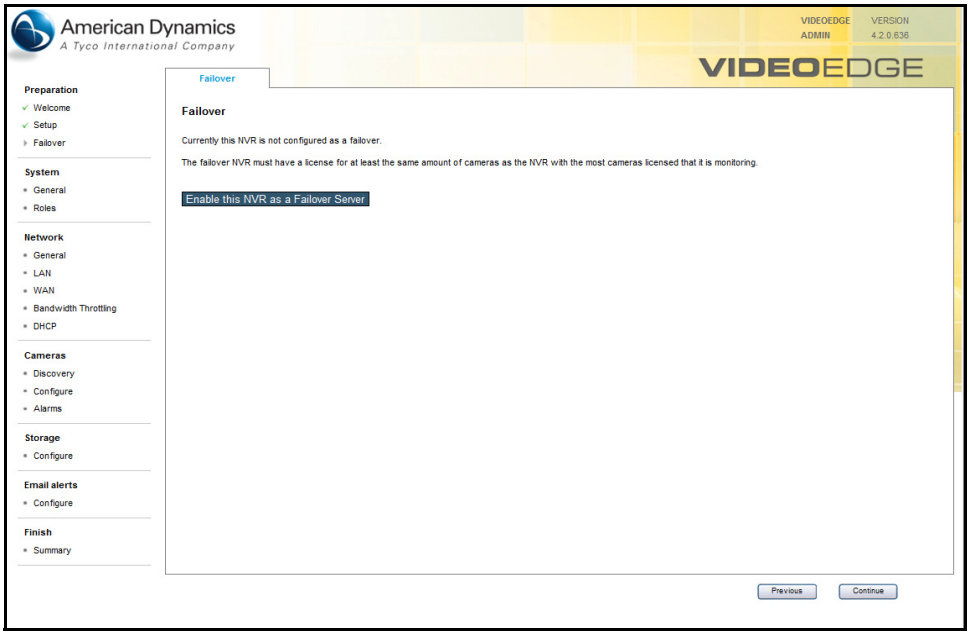
Continue to Procedure 3-15 Failover Settings.

**- End -**

## Failover Page

The Failover page is used to enable the NVR to act as a failover server for one or more NVRs on the network.

**Figure 3-11 Failover Page**




## Procedure 3-15 Failover Settings

| Step | Action |
|---|---|
| 1 | Select **Enable this NVR as a Failover Server** if required.<br>The NVR Failover page opens. |
| 2 | Configure the Failover settings as required. |

3 Select **Continue** to advance to the next page. Continue to Procedure 3-16 System Info Settings.

**Note**

For further information on configuring an NVR as a Failover server refer to Procedure 17-1 Configuring Failover Mode for an NVR on page 179.

**- End -**

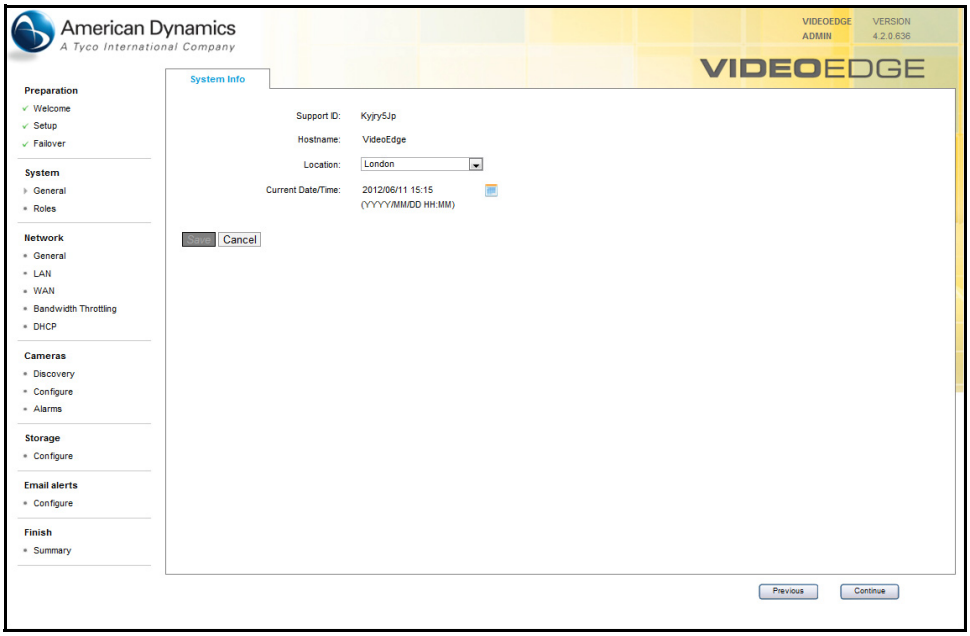
# System

This section describes the system stage of the Setup Wizard including the General and Roles pages.

## System Info Page

The System Info page is used to edit the NVR hostname, location, current date and current time.

**Figure 3-12 System Info Page**




## Procedure 3-16 System Info Settings

| Step | Action |
|---|---|

1 To edit the following fields:

- **Hostname**
- **Current Date/Time**

Select the current value. Edit the value as required.

2 To edit the **Location**, select the city from the dropdown. If your current location is not available select the nearest city that is listed.

3 Edit the setting and click **Save**.

4 Click **Continue** to advance to the next page. Continue to Procedure 3-17 Roles Settings.

**Note**

For further information on General System settings refer to General System Information on page 135.

**- End -**

## Roles Page

The Roles page is used to change the passwords for the admin and operator user accounts.

### Changing the Main Administrator's Password

The main administrator account has complete access to the NVR interface and all its functions and it cannot be deleted.

The main administrator ID is always **admin** and cannot be changed, whereas, the main administrator's password can be, and should be changed. When a NVR is installed for the first time or when the NVR has been restored to factory default settings, the administrator's default credentials are:

ID: **admin**

Password: **VIDEO!edge23**

As this is the default password supplied with all NVRs, there are security risks if you do not change the password to a private password, known only to the administrator and those to whom the administrator is responsible. It is recommended that you change the main administrators password during installation.

### Changing the Operator's Password

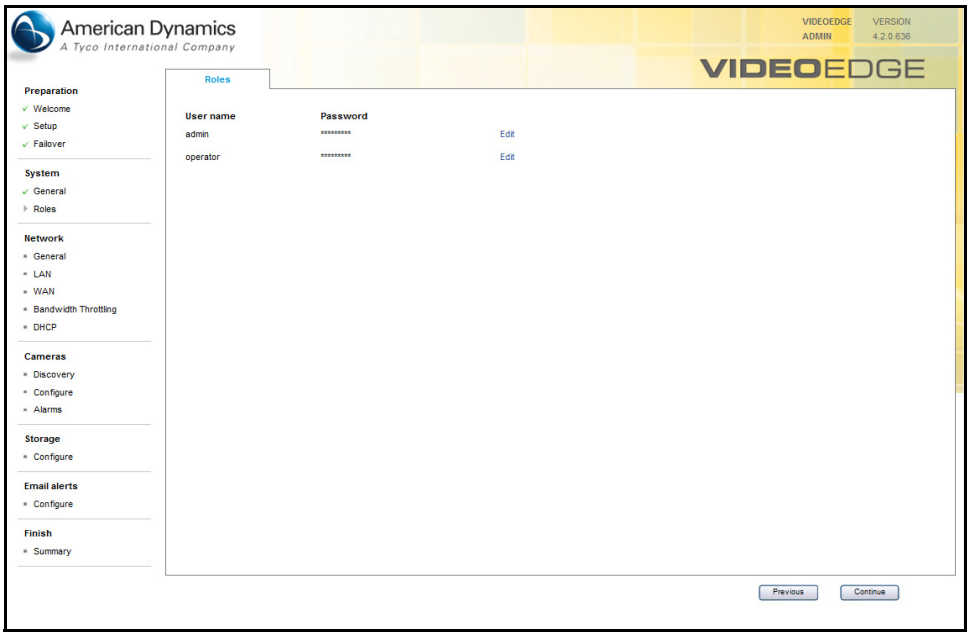
The operator account has access to view video and settings on the NVR interface but not to edit them, it can also not be deleted. It also is unable to view logs which have been generated by the NVR.

The operator ID is always **operator** and cannot be changed, whereas its password can be, and again like the admin account should be changed. When the NVR is first installed the default credentials are as follows:

ID: **operator**

Password: **VideoEdge**

**Figure 3-13 Roles Page**




## Procedure 3-17
## Roles Settings

| Step | Action |
|---|---|
| 1 | To change the password for either the admin or operator user account select **Edit** next to the appropriate username. |
| 2 | Edit the password as required and click **OK**. |
| 3 | Click **Continue** to advance to the next page. Continue to Procedure 3-18 Network General Settings. |

**Note**

For further information on Roles refer to Roles on page 138.

**- End -**

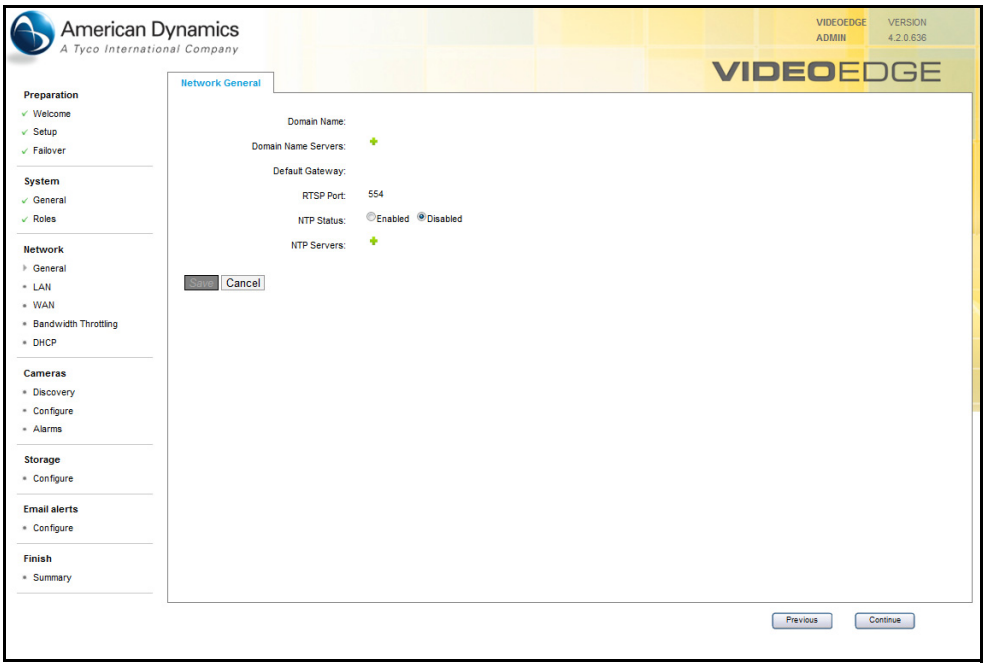
# Network

This section describes the network stage of the Setup Wizard including the General, LAN, DHCP, WAN and Dynamic Bandwidth.

## Network General Page

The General page is used to edit the general network settings including domain name, domain name servers, default gateway, RTSP port, NTP status and NTP servers.

**Figure 3-14 Network General Page**




## Procedure 3-18
## Network General Settings

| Step | Action |
|---|---|
| 1 | To edit the following fields:<br>• **Domain Name**<br>• **Default Gateway**<br>• **RTSP Port**<br>Select the current value. Edit the value as required. |
| 2 | Click **Save**. |
| 3 | To edit the following fields:<br>• **Domain Name Servers**<br>• **NTP Servers**<br>**a** Select the icon.<br>A text box displays<br>**b** Enter the Server addresses in the text box.<br>**c** Click **Save**. |

### Caution

In order to provide reliable playback both the NVR and victor client must be NTP clients of the same NTP server.

4 To edit the NTP Status click either the **Enable** or **Disable** option button.

5 Click **Save/Continue** to advance to the next page. Continue to Procedure 3-19 LAN Interface Settings.

**Note**

For further information on general network settings refer to General Network Settings on page 149.

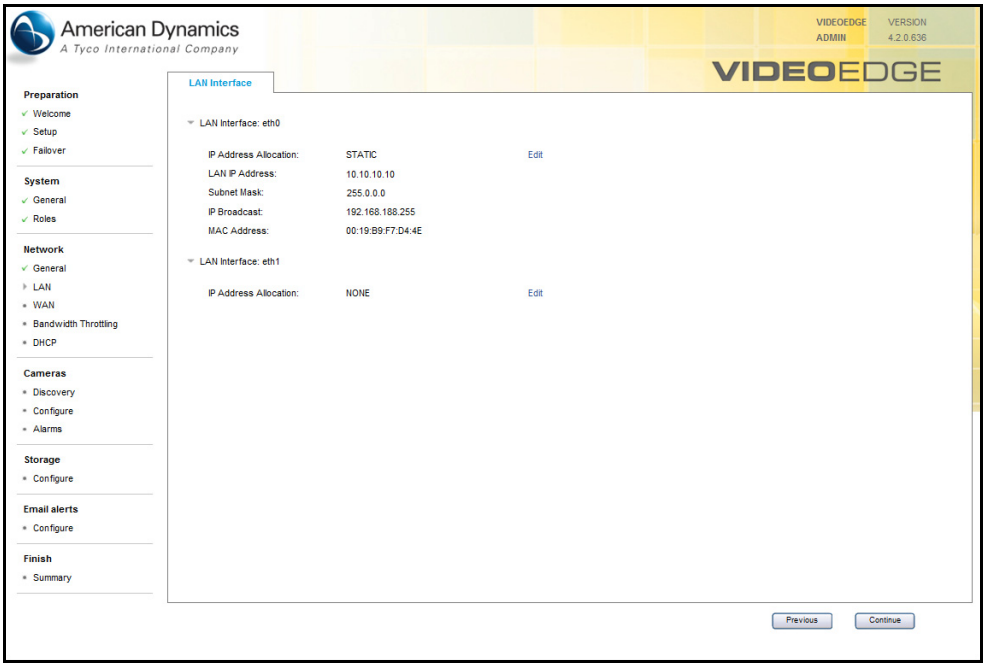
**- End -**

## LAN Interface Page

The LAN page is used to edit the LAN interface settings for each NIC including IP address allocation, LAN IP address, subnet mask and IP broadcast.

The NVR can have multiple active NICs. This allows the use of dedicated camera networks.

**Figure 3-15 LAN Interface Page**




## Procedure 3-19
## LAN Interface Settings

| Step | Action |
|---|---|

1 To edit the LAN Interface settings, select **Edit** next to the NIC you want to modify. You can edit the following fields:

- **IP Address Allocation**

**Note**

To open the NVR Web Interface the IP address of one of the NICs must be known, if all the IP addresses are dynamic they will vary in value. It is recommended that a NIC is configured with a static IP address and subnet mask for this reason.

- **LAN IP address**
- **Subnet Mask**

**Note**

The Subnet Mask is defined by three classes of IP Address A, B and C which will determine its value. They are as follows:

- **Class A** - First Octet Decimal Range 1-126, Subnet Mask Value **255.0.0.0**
- **Class B** - First Octet Decimal Range 128-191, Subnet Mask Value **255.255.0.0**
- **Class C** - First Octet Decimal Range 192-223, Subnet Mask Value **255.255.255.0**

Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and are reserved for loopback and diagnostic functions.

- **IP broadcast**

2 Edit the setting as required and click **Save**.

3 Click **Continue** to advance to the next page. Continue to Procedure 3-20 WAN Settings.

**Note**

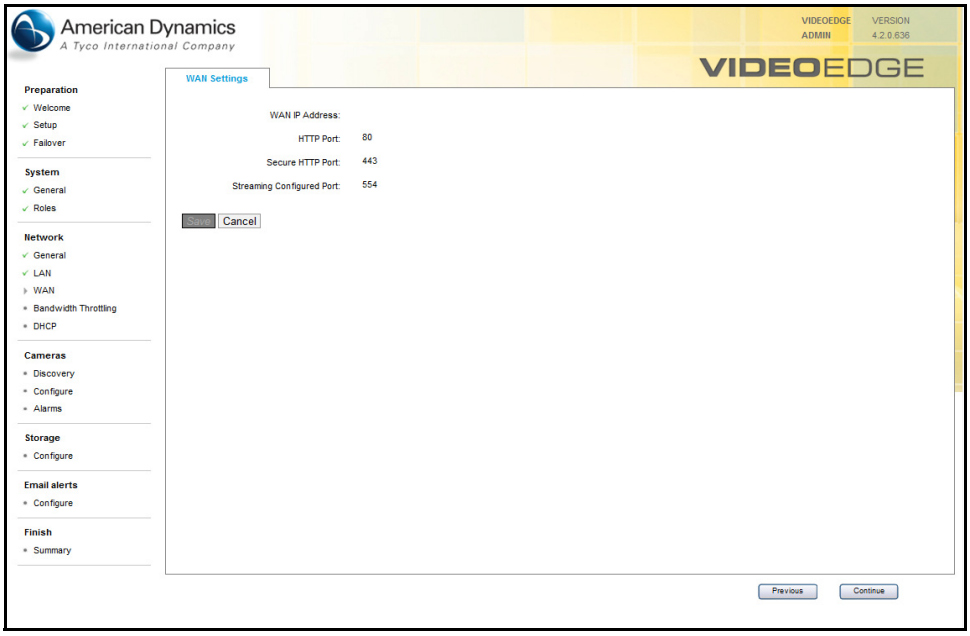
For further information on LAN interface settings refer to Procedure 15-8 Editing the LAN Interface Values on page 154.

**- End -**

## WAN Settings Page

The WAN Settings page is used to edit the WAN settings including the WAN IP address, HTTP port, secure HTTP port and streaming configured port.

**Figure 3-16 WAN Settings Page**




## Procedure 3-20
## WAN Settings

| Step | Action |
|---|---|

**1** To edit the following fields:

- **WAN IP address**
- **HTTP Port**
- **Secure HTTP Port**
- **Streaming Configured Port**

Select the current value. Edit the value as required.

**2** Click **Save**.

**3** Click **Continue** to advance to the next page. Continue to Procedure 3-21 Dynamic Bandwidth Settings.

**Note**

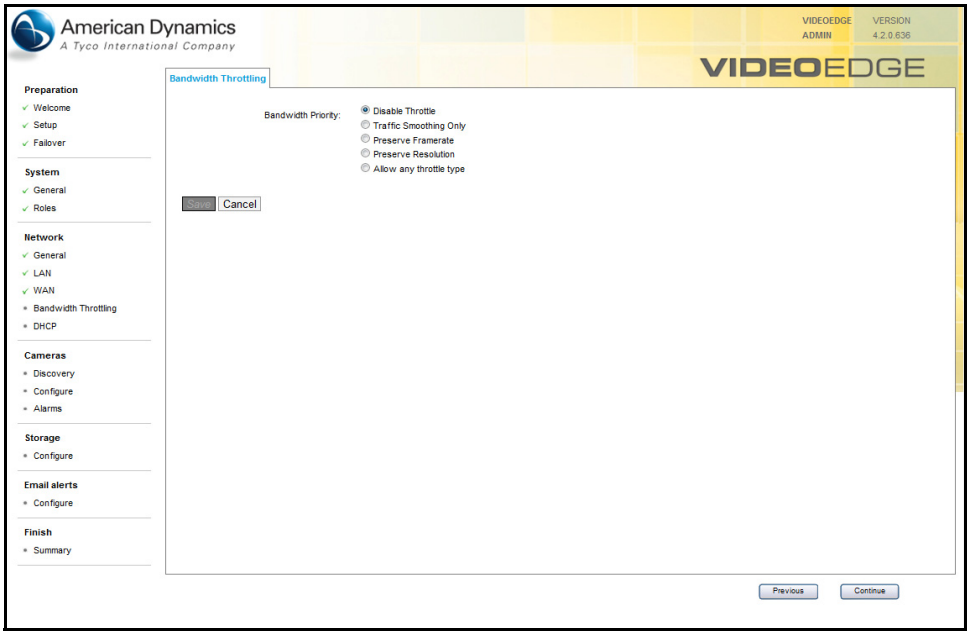
For further information on WAN settings refer to WAN Settings on page 157.

**- End -**

## Dynamic Bandwidth Page

The Dynamic Bandwidth page is used to edit the Bandwidth Throttling settings including Bandwidth Priority, Traffic smoothing, WAN and LAN bitrate caps and Transcode Limit.

**Figure 3-17 Dynamic Bandwidth Page.**




## Procedure 3-21
## Dynamic Bandwidth Settings

| Step | Action |
|---|---|

**1** To edit the following fields:

- **Bandwidth Priority**

Click the required option button.

Which of the available fields display will depend on which Bandwidth Priority option is enabled.

**2** Click **Save**.

**3** To edit the **Traffic Smoothing** values select the current values. Update the values as required.

**4** Click **Save**.

**5** To edit the following fields:

- **WAN Bitrate Cap**
- **LAN Bitrate Cap**

Select the required value from the dropdown.

Or

**a** To use a custom value, select **Custom** from the dropdown.
The custom entry field displays.

**b** To edit the **bitrate cap** value select the current value. Update the value as required.

**c** Enter the desired bitrate cap value in the field.

**Note**

The custom value must be entered in **kbps**. For example to enter a value of 5.5Mbps you would type a value of 5500.

**6** To edit the **Transcode Limit** select the required value from the dropdown.

**7** Click **Save**.

**8** Click **Continue** to advance to the next page. Continue to Procedure 3-22 DHCP Server Settings.

**Note**

For further information on Dynamic Bandwidth settings refer to Bandwidth Priority on page 163.

**- End -**

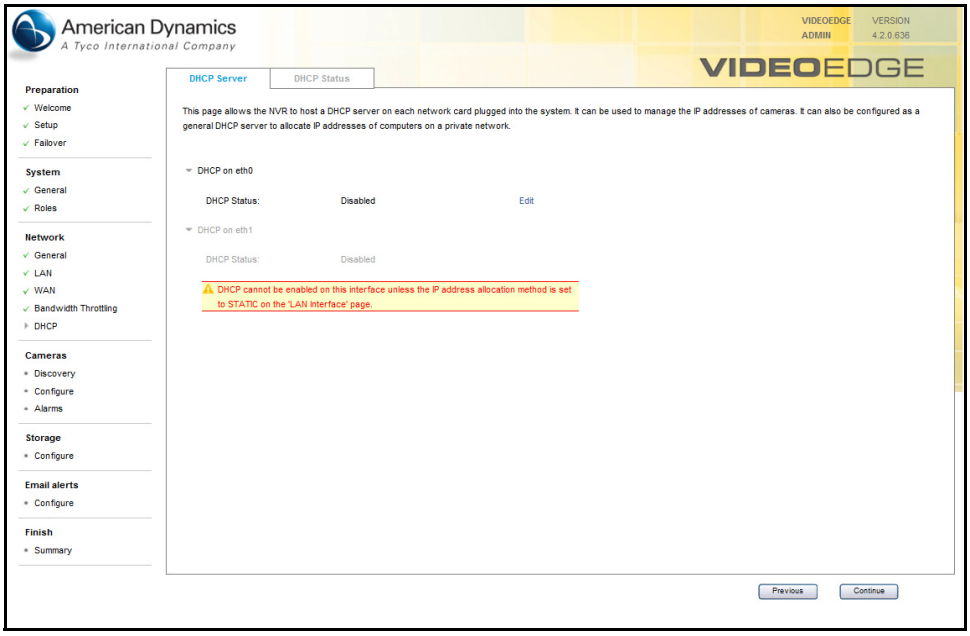
## DHCP Server Page

The DHCP Server page is used to edit the DHCP server settings for each NIC including the DHCP status, start range, end range, subnet and netmask. Each NIC can be used to host a DHCP server for the LAN it is attached to.

If a NIC has been designated a Dynamic IP address it will not be available for editing on this page.

The DHCP Status page allows you to view all active devices which have been assigned a dynamic IP address by the NVR.

**Figure 3-18 DHCP Server Page**




## Procedure 3-22
## DHCP Server Settings

| Step | Action |
|---|---|

**1** To edit the following fields:

- **DHCP Status**
- **Start Range**
- **End Range**
- **Subnet**
- **Netmask**

for each NIC select **Edit** next to the setting.

**2** Edit the setting and click **OK**.

**3** Click **Continue** to advance to the next page. Continue to Procedure 3-23 Discovery Settings.

**Note**

For further information on DHCP Server settings refer to Procedure 15-9 Editing the DHCP Server Settings on page 156.

**- End -**

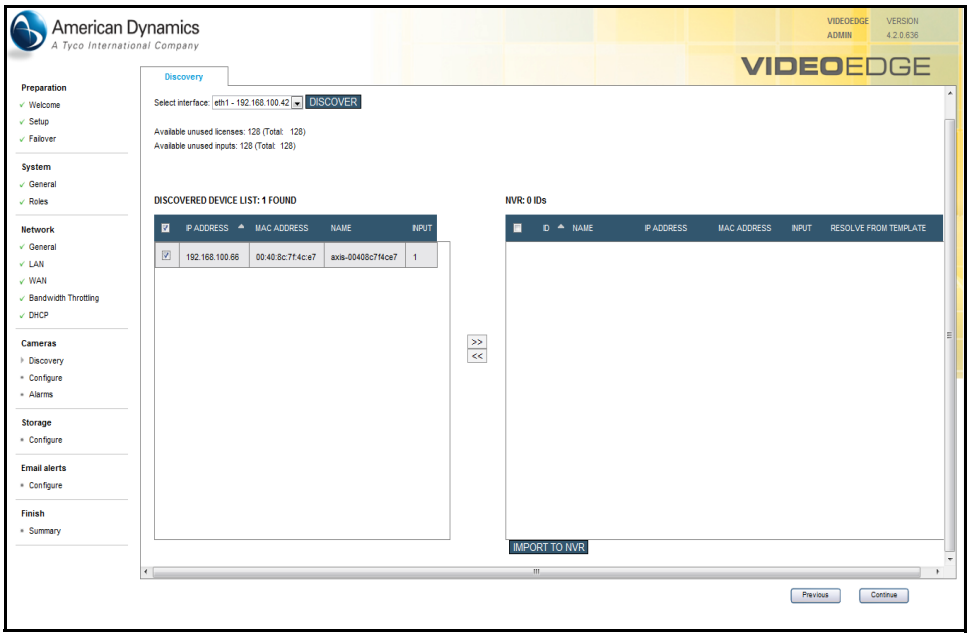
# Cameras

This section describes the cameras stage of the Setup Wizard including the Discovery, Configure and Alarms pages.

## Discovery Page

The Discovery page is used to discover and add IP cameras from selected networks.

**Figure 3-19 Discovery Page**




## Procedure 3-23
## Discovery Settings

| Step | Action |
|---|---|
| 1 | Select the camera network **NIC** from the dropdown. |
| 2 | Select **Discover**.<br>Discovered devices will display in the Discovered Device List. |
| 3 | Select checkbox for cameras you want to add. Use the arrow >> to move selected cameras to the NVR list. |
| 4 | Select the checkbox for the cameras you want to add in the NVR list. |
| 5 | Select **Import to NVR**. |

6 Select **Continue** to advance to the next page. Continue to Procedure 3-24 Camera List Settings.

**Note**

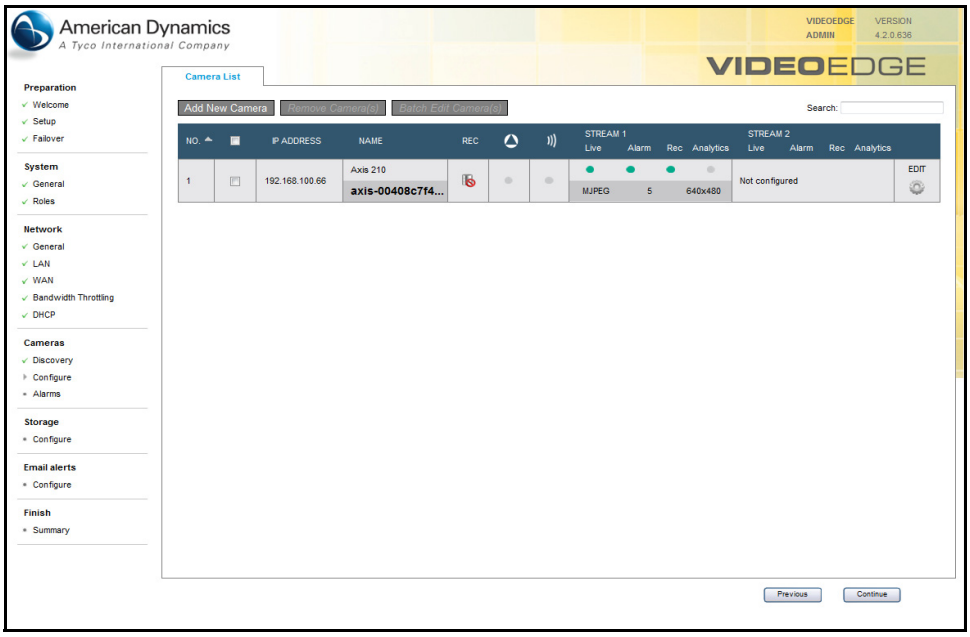
For further information on Camera and Device Discovery refer to Procedure 7-5 Adding Cameras using Auto-Discovery on page 83.

**- End -**

## Camera List Page

The Camera List page is used to manually add IP cameras and devices to the NVR.

**Figure 3-20 Camera List Page**




## Procedure 3-24
## Camera List Settings

| Step | Action |
|---|---|
| 1 | Select **Add New Camera**.<br>Add Camera Window opens. |
| 2 | Enter camera name in the **Camera Name** textbox. |
| 3 | Enter the cameras IP address in the **Internal IP Address** textbox. |

4 Select the **Password Group** from the dropdown list.

**Note**

The **Password Group** will usually be default. The NVR will use the manufacturers default password to connect to the camera. However, if you have changed the password for this camera, you need to assign the camera to the appropriate password group, or create a new password group. For further information on password groups refer to Camera Password Groups on page 131.

5 (Optional) If multiple storage sets are defined, select the **Storage Set** from the dropdown list.

6 Select **Apply**.

7 Select **Continue** to advance to the next page. Continue to Procedure 3-25 Alarms Settings.

**Note**

For further information on adding cameras manually refer to Procedure 7-4 Manually Adding an IP Camera or Encoder on page 81.

**- End -**

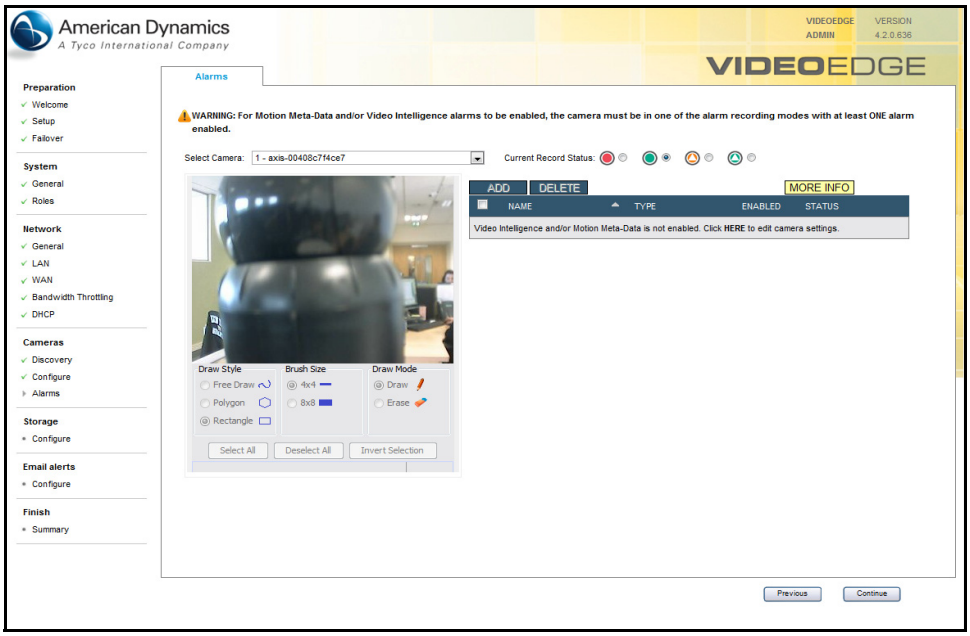
## Alarms Page

The Alarms page is used to configure Video Intelligence and Motion Detection alarms for individual cameras. Motion Detection or Video Intelligence must be enabled on each camera for which you wish to configure alarms.

**Note**

This stage is not available when using Firefox on the local machine.

**Figure 3-21 Alarms Page**




## Procedure 3-25
## Alarms Settings

| Step | Action |
|---|---|
| 1 | Select the camera you want to add an alarm to from the **Select Camera** dropdown menu. |
| 2 | Select the **Current Record Status** for the camera. |
| 3 | Select **Add**. |
| 4 | Define the camera alarm and select **Save**. |

**Note**

Depending on the camera's settings you can select Motion Detection or Video Intelligence alarms.

| | |
|---|---|
| 5 | Click **Continue** to advance to the next page. Continue to Procedure 3-26 Basic Settings. |

**Note**

For further information on the Motion Detection and Video Intelligence refer to Motion Detection on page 103 and Video Intelligence on page 113.

**- End -**

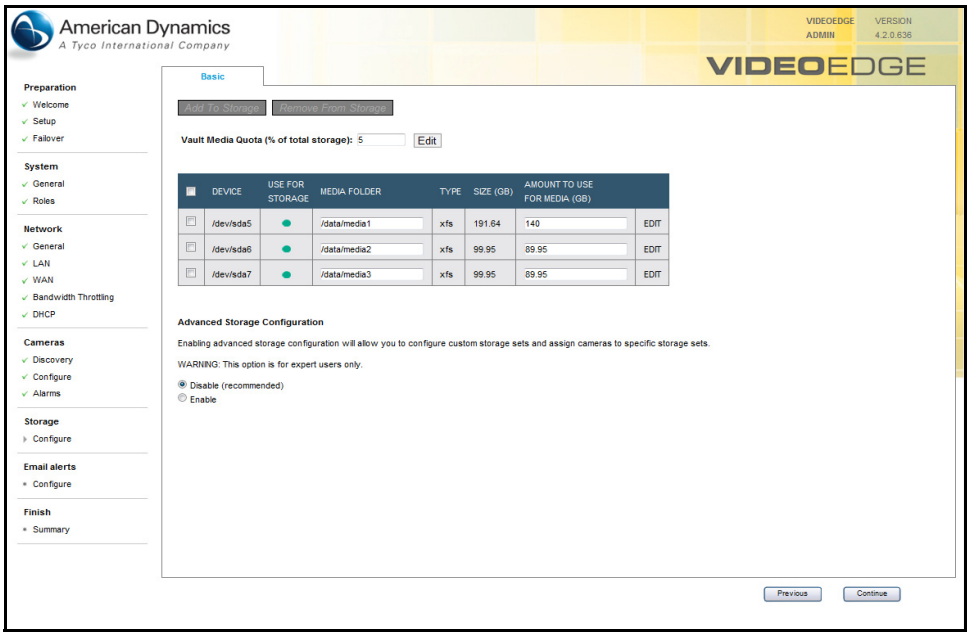
# Storage

This section will describe the storage stage of the Setup Wizard.

## Basic Page

The Basic page is used to edit storage settings including the vault media quota and whether advanced storage configuration is enabled.

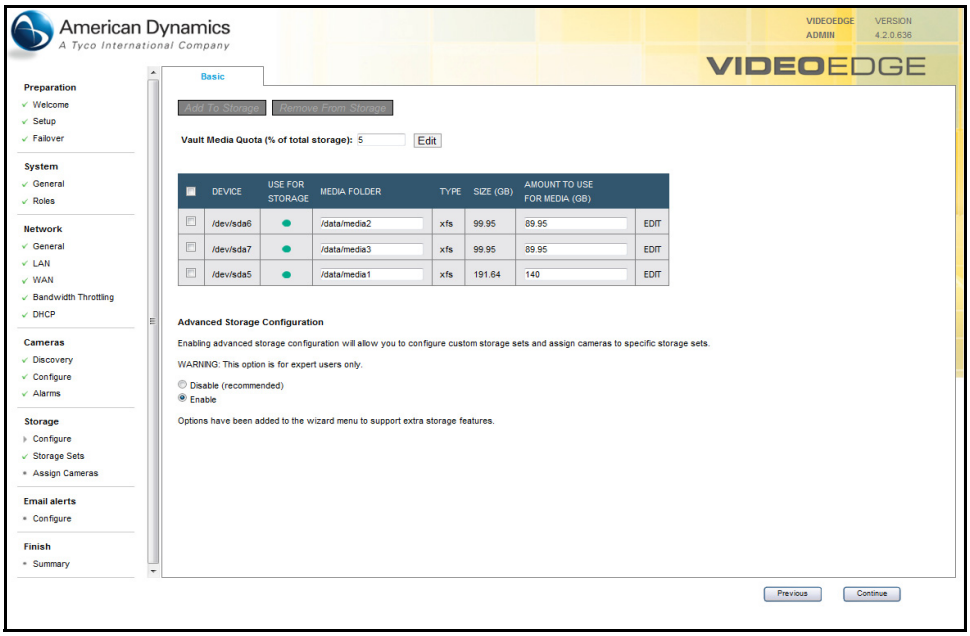
**Figure 3-22 Basic Page**




## Procedure 3-26
## Basic Settings

| Step | Action |
|---|---|
| 1 | To edit the Vault Media Quota select **Edit**, then enter the desired percentage of storage to be allocated as the **Vault Media Quota** in the text box. |
| 2 | Select **Apply Quota**. |
| 3 | To add drives to storage, select the check boxes for each desired drive, then click **Add to Storage**. |
| 4 | (Optional) Select to the **Enable** Advanced Storage configuration option button.<br>Two additional steps are added to the wizard; **Storage Sets** and **Assign Cameras**. |

**Figure 3-23 Basic Page with Advanced Storage Configuration Enabled**




**Note**

Enabling advanced storage allows you to create storage sets and to assign media folders of cameras to the created storage sets.

**5** Click **Continue** to advance to the next page.

If advanced storage configuration is enabled continue to Storage Sets Page.

Or

If advanced storage configuration is disabled continue to Procedure 3-29 Email Alerts Settings.

**Note**

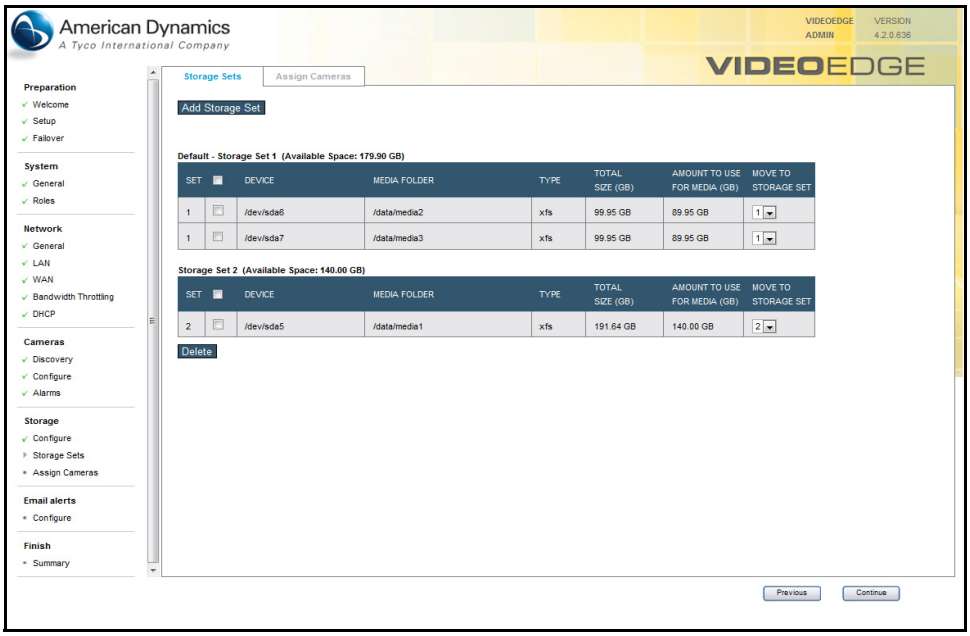
For further information on assigning cameras manually to storage sets refer to Procedure 5-7 Reassigning a Camera to a Different Storage Set on page 69.

**- End -**

## Storage Sets Page

The Storage Sets page allows you to create custom storage sets from the media folders which were created during the Configuring Storage Partitions stage of the installation.

**Figure 3-24 Storage Sets Page**




## Procedure 3-27
## Storage Set Settings

| Step | Action |
|---|---|
| 1 | Click **Add Storage Set** to create a new storage set. |
| 2 | Use the checkboxes to select media folders. |
| 3 | Use the **Move to Storage Set** dropdown to select the storage set you wish to move the media folders to. |
| 4 | Click **Continue** to advance to the next page. Continue to Procedure 3-28 Assign Cameras Settings |

**Note**

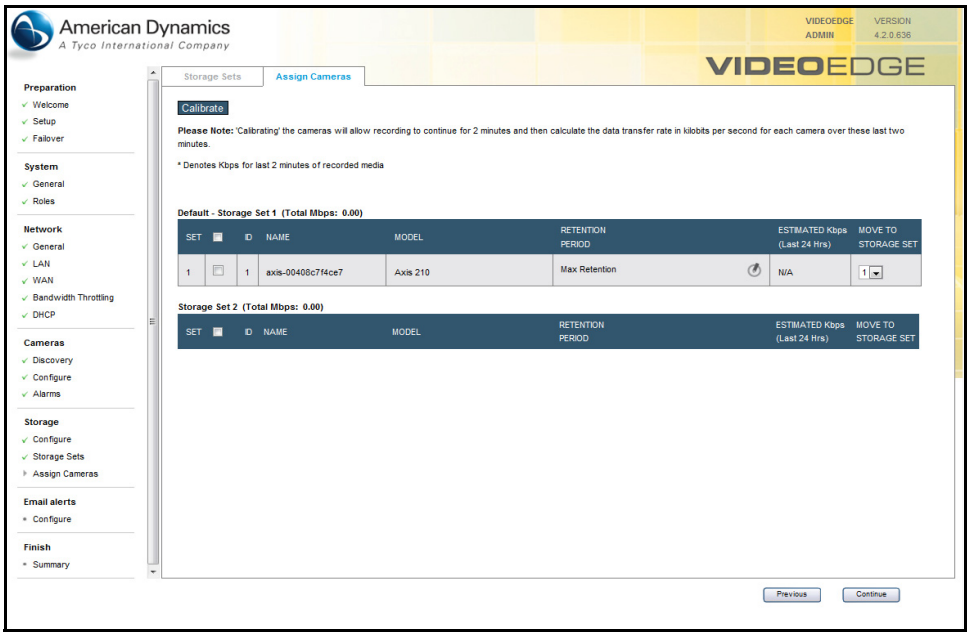
For further information on assigning cameras to storage sets refer to Media Folder Assignment for Storage Sets on page 68.

**- End -**

## Assign Cameras Page

The Assign Cameras page allows you to assign cameras to different storage sets to best suit your storage specifications. You can also calibrate each camera to calculate its data transfer rate which you can use to determine the best storage set to assign it to.

**Figure 3-25 Assign Cameras Page**




## Procedure 3-28
## Assign Cameras Settings

| Step | Action |
|---|---|
| 1 | Use the checkboxes to select the cameras you wish to calibrate. |
| 2 | Click **Calibrate**.<br>Calibration will allow the cameras to record for 2 minutes. |
| 3 | Use the **Move to Storage Set** dropdown to select the storage set you wish to move the camera to. |
| 4 | Click **Continue** to advance to the next page. Continue to Procedure 3-29 Email Alerts Settings |

**Note**

For further information on assigning media folders to storage sets refer to Assigning Cameras to Storage Sets on page 68.

**- End -**

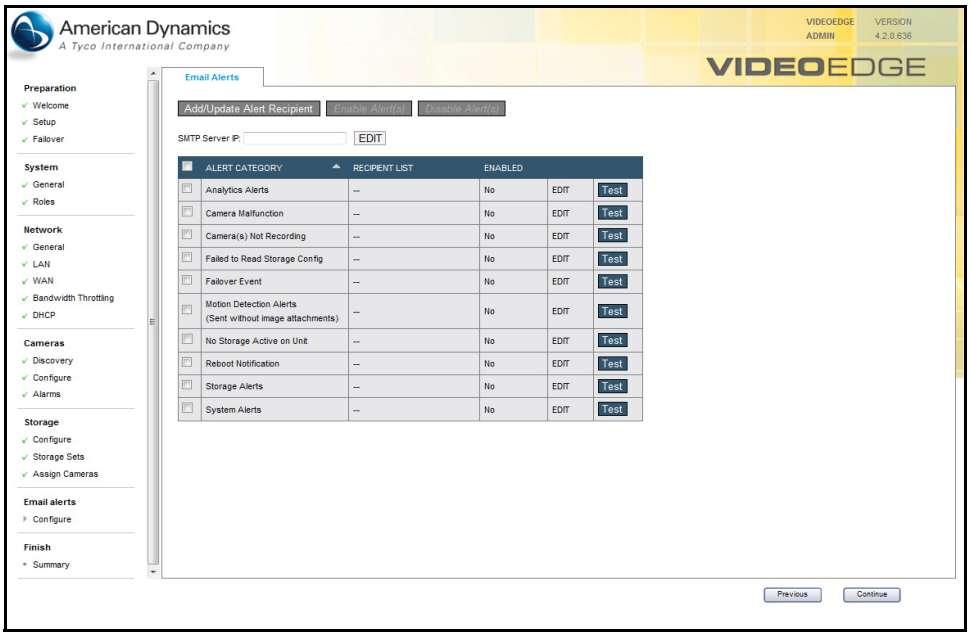
# Email Alerts

This section describes the email alerts stage of the Setup Wizard.

## Email Alerts Page

The Email Alerts page is used to assign a SMTP server address, add recipients to receive email alerts, edit the alerts received by each recipient and enable/disable alert types.

**Figure 3-26 Email Alerts Page**




## Procedure 3-29
## Email Alerts Settings

| Step | Action |
|---|---|
| 1 | Enter the IP address in the **SMTP Server IP** text box. |
| 2 | Click **Add/Update Alert Recipient**. |
| 3 | Click the **New Recipient Email Address** option button and enter a recipient email address in the field and/or click the **Use Recipient Email Address** option button and select an already entered address from the dropdown. |
| 4 | Select the **Alert Categories** to be assigned to the address(es) using the check boxes. |
| 5 | Click **Save**. |
| 6 | Select the **Alert Category** check boxes. |
| 7 | Click **Enable Alert(s)**. |
| 8 | Click **Test** next to an alert category to send a test email alert. |

9 Click **Continue** to advance to the next page. Continue to Procedure 3-30 Completing the NVR Setup.

**Note**

For further information on email alerts refer to Email Alerts on page 209.

**- End -**

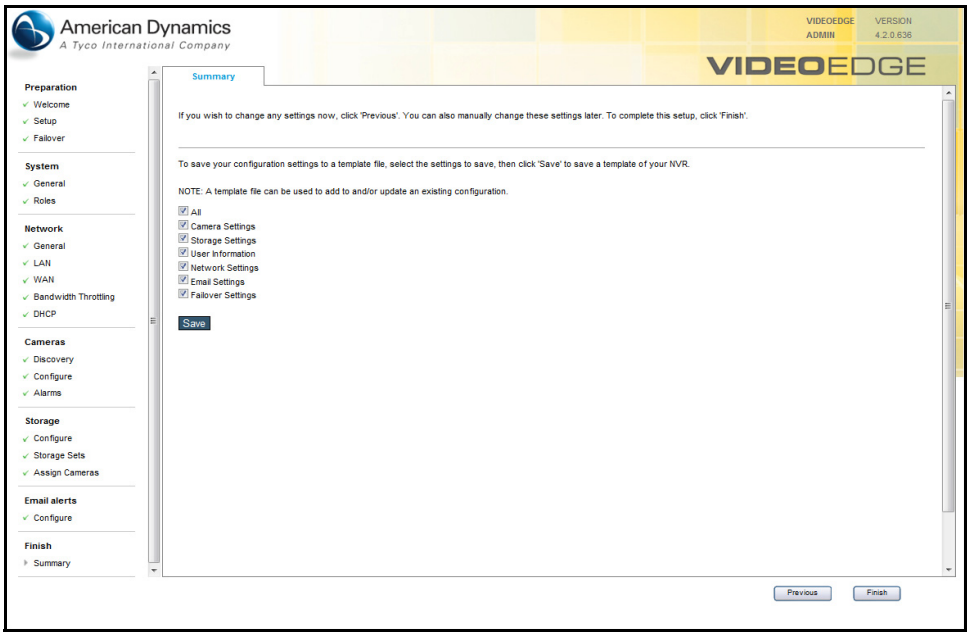
# Finish

This section allows you to save a template of the current NVR settings. These can then be used if the NVR is reinstalled or used to quickly configure another NVR with these settings.

## Summary Page

The Summary page is used to save a settings template file prior to finishing the setup process. A saved template can be used in the future to set up an NVR with these settings.

**Figure 3-27 Summary Page**




## Procedure 3-30 Completing the NVR Setup

| Step | Action |
|---|---|
| 1 | Select the checkboxes for the template settings you want to save. |
| 2 | Click **Save**. |
| 3 | Select **Save As**. |

4 Navigate to the folder where you want to save the template.

5 Enter a **File name** for the template and click **Save**.

6 Click **Finish** to complete the Setup Wizard or click **Previous** to go back.

**Note**

For further information on templates refer to NVR Failover, Configuration Backup, Templates and Updates on page 177.

**- End -**

# Using the NVR Interface

## Overview

The NVR interface allows users to interact with the NVR. This provides information about the server and allows you to modify the server's settings. The NVR interface is accessible via a web client or through victor unified client. All pages on the web client are static. You must refresh your browser to keep all information current.

To access the web client, you must know its IP address and have a User name and Password combination that is valid for the NVR.

A workstation logging into the NVR using the web interface must have Java 6 or above installed. If the workstation is connected to the Internet, but does not have Java installed, you must download Java from its website http://www.java.com. You must also enable javascript on your browser.

To access the NVR through victor unified client, you must add the NVR Recorder to your recorders in the device list in victor client. For information on how to add the NVR recorder to victor refer to Setting Up Recorder Devices in the victor Configuration and User Guide.

This chapter explains how to log into the NVR Server Web Interface, access the NVR configuration via victor unified client and provides an overview of the user interface.

## Logging into the NVR Server Web Interface

To access the NVR Web Interface you must log in. There are two user accounts, **System Administrator** and **Operator**.

If you log in using a **System Administrator** account you will have access to configure and edit all settings of the NVR. If you log in using a **Operator** account, you do not have permissions to edit any of the settings, you can only view the current settings and view live video.

### Procedure 4-1
### Logging into the NVR Server Web Interface

| Step | Action |
|---|---|
| **1** | Launch your web browser and enter the NVR IP address into the **URL** field. |

Enter **http://NVR_Server_IP_Address**, where **NVR_Server_IP_Address** is the IP address of the machine running the NVR software, for example, **http://192.187.100.21**

**2** The NVR login dialog box opens. Enter your **User name** and **Password**.

User name: **admin**

Default Password: **VIDEO!edge23**

Or

User name: **operator**

Default Password: **VideoEdge**

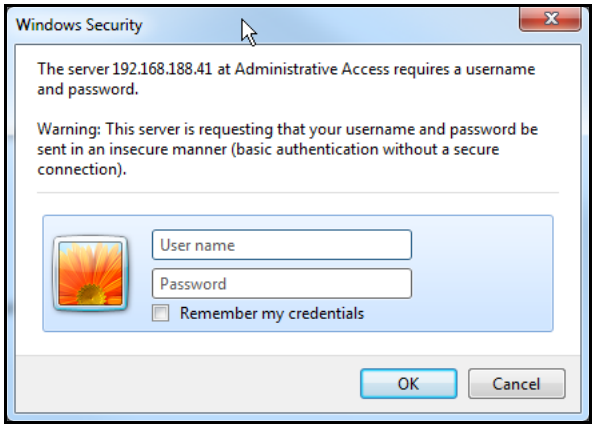
**Note**

1 You are asked to login/authenticate when you:

- First log on to the NVR Web Server.
- Are already logged on and your user access is changed.

2 If you have changed the account passwords, use these in place of the default password.

**Figure 4-1 NVR Login Dialog**


Windows Security
The server 192.168.188.41 at Administrative Access requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name
Password
Remember my credentials
OK
Cancel

**3** Click **OK**.

The web page interface for the NVR opens (Figure 4-3).

**- End -**

# victor NVR Configuration Interface

To access the victor NVR configuration interface you must have the NVR added as a recorder in the device list on your victor client. For information on how to add the NVR recorder to victor refer to the victor Configuration and User Guide.

By configuring the NVR through victor you can configure your NVR in exactly the same way as via the web interface. However, when using victor you do not have the option to view live video. Instead use the **Surveillance** pane in the victor client to view NVR cameras in live mode.

## Procedure 4-2
## Accessing the victor NVR Configuration Interface

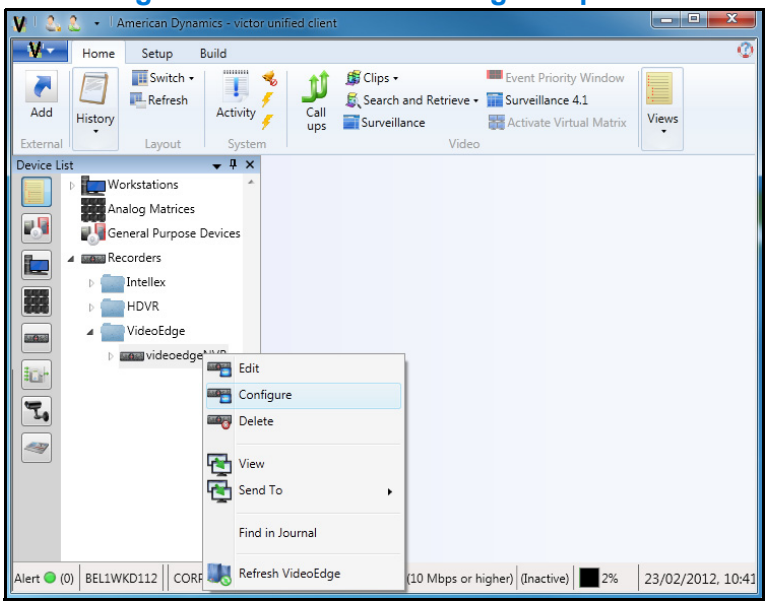
| Step | Action |
|---|---|

**1** In the victor client, expand **Recorders** in the Device List.

**2** Expand the **VideoEdge** folder.

**3** Right-click on the NVR recorder you want to configure.

**Figure 4-2 victor NVR Configure option.**

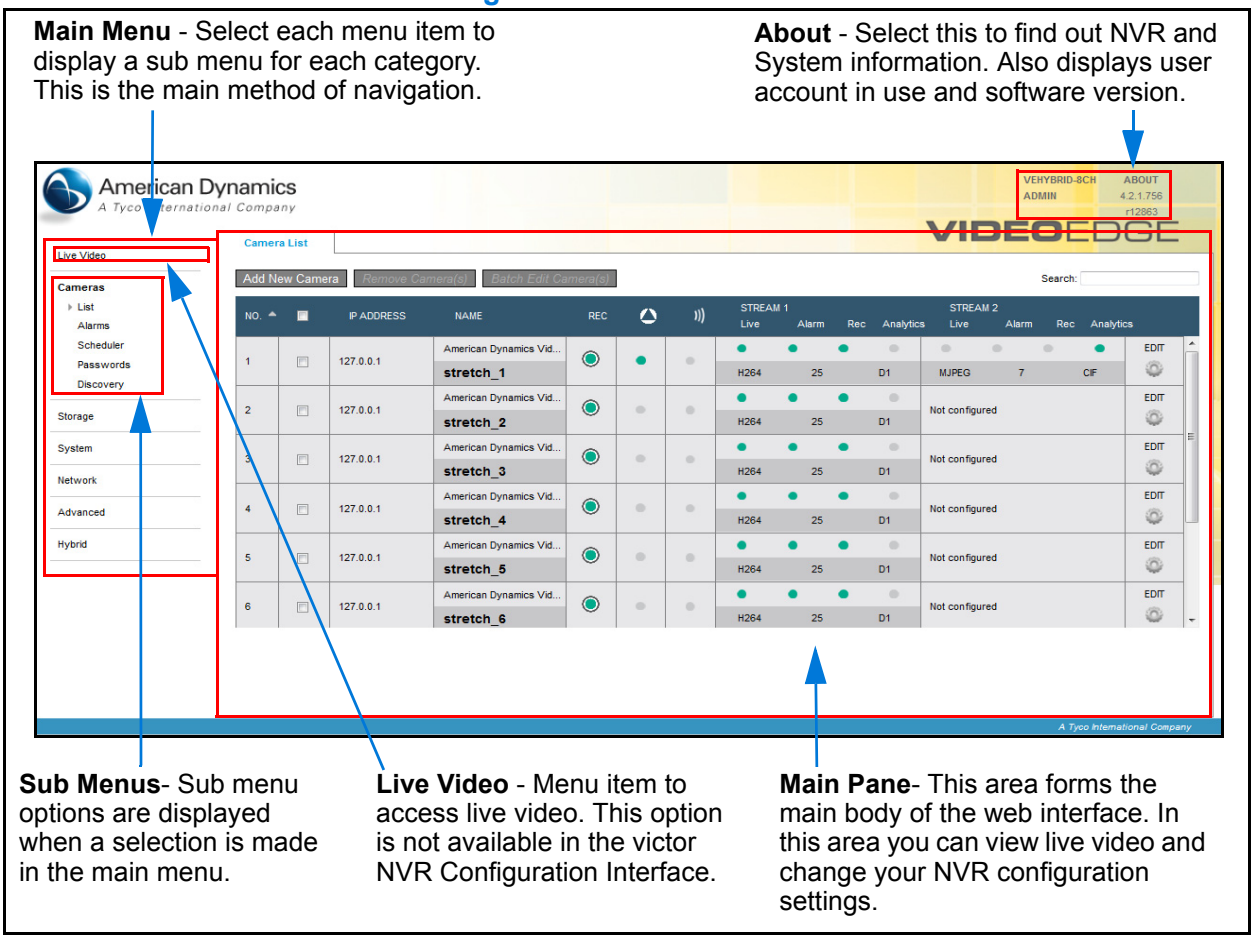



**4** Select **Configure**.

The NVR configuration interface opens (Figure 4-3).

**- End -**

**Figure 4-3 NVR Interface**


**Main Menu** - Select each menu item to display a sub menu for each category. This is the main method of navigation.
**About** - Select this to find out NVR and System information. Also displays user account in use and software version.
American Dynamics
A Tyco International Company
VEHYBRID-8CH
ADMIN
ABOUT
4.2.1.756
r12863
VIDEOEDGE
Live Video
Cameras
List
Alarms
Scheduler
Passwords
Discovery
Storage
System
Network
Advanced
Hybrid
Camera List
Add New Camera
Remove Camera(s)
Batch Edit Camera(s)
Search:
NO.
IP ADDRESS
NAME
REC
STREAM 1
STREAM 2
Live
Alarm
Rec
Analytics
EDIT
1 127.0.0.1 American Dynamics Vid... stretch_1 H264 25 D1 MJPEG 7 CIF
2 127.0.0.1 American Dynamics Vid... stretch_2 H264 25 D1 Not configured
3 127.0.0.1 American Dynamics Vid... stretch_3 H264 25 D1 Not configured
4 127.0.0.1 American Dynamics Vid... stretch_4 H264 25 D1 Not configured
5 127.0.0.1 American Dynamics Vid... stretch_5 H264 25 D1 Not configured
6 127.0.0.1 American Dynamics Vid... stretch_6 H264 25 D1 Not configured
A Tyco International Company
**Sub Menus**- Sub menu options are displayed when a selection is made in the main menu.
**Live Video** - Menu item to access live video. This option is not available in the victor NVR Configuration Interface.
**Main Pane**- This area forms the main body of the web interface. In this area you can view live video and change your NVR configuration settings.

# Navigating the NVR Interface

To navigate the NVR Interface and access the required configuration settings, use the menu and sub menus down the left of the page.

The menu is divided into several main areas:

- **Live Video** (web interface only)
- **Cameras**
- **Storage**
- **System**
- **Network**
- **Advanced**

Each menu is further divided into sub menus for easy navigation to the required configuration settings.

## Live Video Menu

The Live Video menu item is only available through the NVR server web interface. This section has sub menus; **1 Camera View** and **2x2 Camera View** .

The Camera View pages allow you to view, either 1 camera or up to 4 cameras simultaneously that are connected to the NVR. From here you can also edit configuration settings for the selected camera.

## Cameras Menu

The Cameras menu has sub menu items; **List**, **Alarms**, **Scheduler**, **Passwords** and **Discovery**.

- **List** - From here you can view a list of all cameras connected to the NVR and view a summary of their configuration status. You can add and remove cameras or edit/batch edit cameras configuration settings.
- **Alarms** - You can create camera alarms, these may be for specific regions of a cameras view. You can also select different types of alarm trigger, for example Motion Detection or Video Intelligence.
- **Schedules** - The scheduler allows you to specify the recording mode (including no recording) that is active at scheduled times during the day.
- **Passwords** - The passwords page allows you to create and maintain camera password groups.
- **Discovery** - This section allows you to use auto-discovery to add cameras to the NVR.

## Storage Menu

The Storage menu has sub menu items; **Basic** and **Advanced**. Use the **Basic** storage configuration option to assign devices available on the NVR as storage devices, edit media folder settings of storage devices, and to allocate a vault media quota. Use the **Advanced** configuration options to assign storage devices and cameras to Storage Sets.

## System Menu

The System menu has sub menu items; **General**, **Roles**, **Licensing**, **Templates**, **Backup/Restore** and **Update Software**.

- **General -** Use to configure and edit general system information.
- **Roles** - Use to edit role password settings.
- **Licensing -** Use to view your VideoEdge NVR license information, apply a license or upgrade your license.
- **Templates** - Sub menu consists of two pages. Use the **Save Template** page to create a custom template based on the settings that are currently configured within the NVR, these include Camera Settings, Storage Settings, User Information, Network Settings, Email Settings and Failover Settings. Use the **Import Template** page to apply an existing template file to the NVR which will edit its settings accordingly.
- **Backup/Restore** - Sub menu consists of two pages. Use the **Backup** page to create a backup of the Camera settings, System Settings, User information, DHCP Settings and NTP Settings. Use the **Restore** page to upload a backup file to restore the NVR settings to the configuration of that Backup file.
- **Update Software** - Use to browse and upload a software upgrade package.

## Network Menu

The Networks menu has menu items; **General**, **LAN Interface**, **DHCP Server**, **WAN Settings** and **Dynamic Bandwidth**.

- **General** - Use to configure general network settings such as the Domain Name, Domain Name Servers, Default Gateway, RTSP Port, NTP Status and NTP Servers.
- **LAN Interface** - Use to configure the available LAN interfaces. Each interface provides the option to configure the IP Address allocation, LAN IP Address, Subnet Mask and IP Broadcast Address. If IP Address allocation is set to either **None** or **DHCP** you will be unable to edit any of the entry fields. The menu will also display the MAC Address of each Network Interface Controller (NIC) for information purposes.
- **DHCP Server** - Use the **DHCP Server** page to configure the DHCP Status for each NIC. The start and end range of the IP Addresses to be included for each NIC during automatic searches for IP Devices can also be configured. Use the **DHCP Status** page to view active devices which have been assigned an IP address by the NVR when it is acting as a DHCP server.
- **WAN Settings** - Used to configure the NVR for operation on a Wide Area Network. In the WAN Settings you can configure the WAN IP Address, HTTP Port, Secure HTTP Port and the Streaming Configured Port.
- **Dynamic Bandwidth** - Use to configure bandwidth throttling, when disabled there is no framedropping or transcoding invoked. In the bandwidth throttling settings you can enable Transcode, select the number of streams to be transcoded, up to four, select the Bandwidth Priority, Traffic smoothing, LAN and WAN bitrate caps.

## Advanced Menu

The Advanced Menu has sub menu items; **Failover**, **Storage Statistics**, **Logs**, **Dark Image Detection**, **Email Alerts, Connected Clients, Reset to Factory Defaults** and **Shutdown.**

- **Failover** - Use to configure the NVR to take over the camera and system settings of another NVR on the network should it fail.
- **Storage Statistics** - Use the **Rec Performance** page to view a graph plotting the recording performance of each storage set. Use the **Rec Statistics** page to view a table of information relating to the recording process of each camera added to the NVR. Use the **Disk Activity** page to view a graph plotting the disk activity for a specific media folder over a specific time period. Use the **Storage Statistics** page to view storage statistics for each Storage Set, Device and Camera.
- **Logs** - Use the **Retrieve Logs** page to customise the search criteria for retrieving log files, the criteria includes date and time range searches, options to retrieve camera logs, recording pipeline descriptions, camera firmware details and core files. The maximum size of the camera log file can be selected from a predefined dropdown list. The **FTP Log Management** page provides the option to upload log files to an FTP server. The **Event Logs** page is used primarily by American Dynamics technical support for troubleshooting. It displays informational and error-related events that have occurred on the NVR system. The **Connection** page displays the Camera Connection Errors that have occurred. The **Camera Logs** page provides information on camera reboots, changed to camera recording status, and the use of Pan-Tilt-Zoom (PTZ) and other controls. The **Audit Trail** page provides information on changes which have been made by a privileged user including; system date/time, software upgrade, FTP log management, user login passwords and network settings.
- **Dark Image Detection -** Use to determine if a camera on the NVR is recording a very dark or potentially black video. Once configured the test will run for each camera on the server once every minute.
- **Email Alerts** - Use the **Email Alerts** page to add email addresses to receive a number of predefined alerts. The **Alert Logs** page displays a log of email alerts which have been transmitted from the NVR.

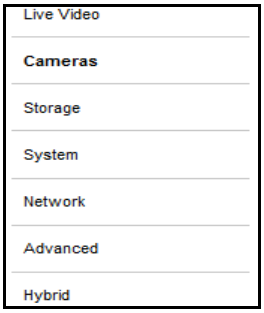
- **Connected Clients** - Use to display the IP Address of the device viewing the NVR via a client, for example, victor unified client or QuickTime. An entry for each camera being viewed from the NVR is displayed with the corresponding IP Address, client type and streaming protocol.
- **Reset to Factory Defaults** - Use to reset the following of the NVR's settings; **Storage**, **Failover**, **User Passwords** and **Alarm** settings. **Saved Media files (video/audio)** can be erased, retained or retained and re-indexed. Carrying out a Reset to Factory Defaults will have no affect on the NVR's Linux based operating system.
- **Shutdown** - Use to Restart NVR Services, Reboot the NVR and to Shutdown the NVR.

## Procedure 4-3
## Navigating the NVR Interface

| Step | Action |
|---|---|

**1** Select the required menu item from the main menu on the left-hand side of the page.

**Figure 4-4 Main Menu**



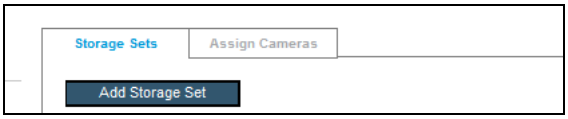

The selected menu item expands to display a sub menu list of items.

**2** Select the required item from the sub menu list.

The relevant configuration settings are displayed in the main pane of the window.

**3** (Optional) Select the tabs at the top of the main pane to navigate between pages.

**Figure 4-5 Tabs on Main Pane.**




**- End -**

# Configuring Storage

## Overview

NVRs can require a tremendous amount of storage space depending on the number of cameras, codec, resolution, and frame rates, recording modes, and the duration for which you wish to preserve video recordings. At the outset of your use of the NVR system, you will need to have storage configured to record data. From time to time, you may find it necessary to replace or add a storage device to produce a greater capacity for video storage.

This chapter describes how to configure storage devices that are physically connected to the NVR and storage devices that are networked to the NVR over a TCP/IP connection.

There are two main storage configuration types, basic and advanced configuration. Basic configuration is the default configuration type where all storage devices and cameras are contained within one storage set. By using advanced storage configuration, you can create numerous storage sets and assign storage devices and cameras to storage sets as required to optimize disk performance. In the Basic storage page, all devices are listed. In the Advanced storage page you can view all the

### Overview of Storage Sets

A storage set is a group of storage devices. One storage set is set up by default on an NVR. This is storage set 1. Initially the default storage set has all enabled storage devices, their media folders and cameras assigned to it, see Figure 5-1 Basic Storage Configuration on page 61.

A Media Folder is a location on a device where media can be recorded to. Media stored in these folders can include video, audio and analytic media. You can only have one media folder per storage device. You can choose which media folders on devices are to be used for storage.

Video from the cameras assigned to a particular storage set will record to the media folders on the storage devices that are assigned to the same storage set.

You can easily create additional storage sets and configure them as required to optimize the disk performance, as media can be recorded to storage sets in parallel.

Each storage set must have at least one assigned media folder for storage. You can assign multiple media folders and cameras to a storage set. It is recommended that you assign no more than 32 devices or cameras to a particular storage set.

## Verifying Storage Devices

The Virtual Disks (aka LUNs or Volumes) may have all been detected by the NVR, but not necessarily configured for usage by the NVR. Ensure that your devices are listed in the Devices list on the Basic Storage Configuration page before moving on to the next section. If any expected storage is missing from the Basic Storage Configuration page, then it is either physically disconnected, the storage device is not recognized due to improper configuration or lack of device driver support, and/or experiencing a storage hardware problem. This may also occur if the filesystem is not mounted.

**Caution**

If you are using RAID storage systems, you must create disk groups and virtual disks on your RAID hardware before setting up storage on the NVR. If you are not familiar with RAID configuration, refer to your storage system's user manual for more information.

## Basic Storage Configuration

Basic storage configuration is the default storage configuration type. Basic storage configuration is the configuration of media folders to be used for recording. All storage devices discovered by the NVR are listed in the default storage set. All cameras added to the NVR are also automatically assigned to the default storage set. You can select which media folders you want to use for media storage, and set the amount of space available to store media. Table 5-1 below describes fields used for basic storage configuration.

**Figure 5-1 Basic Storage Configuration**

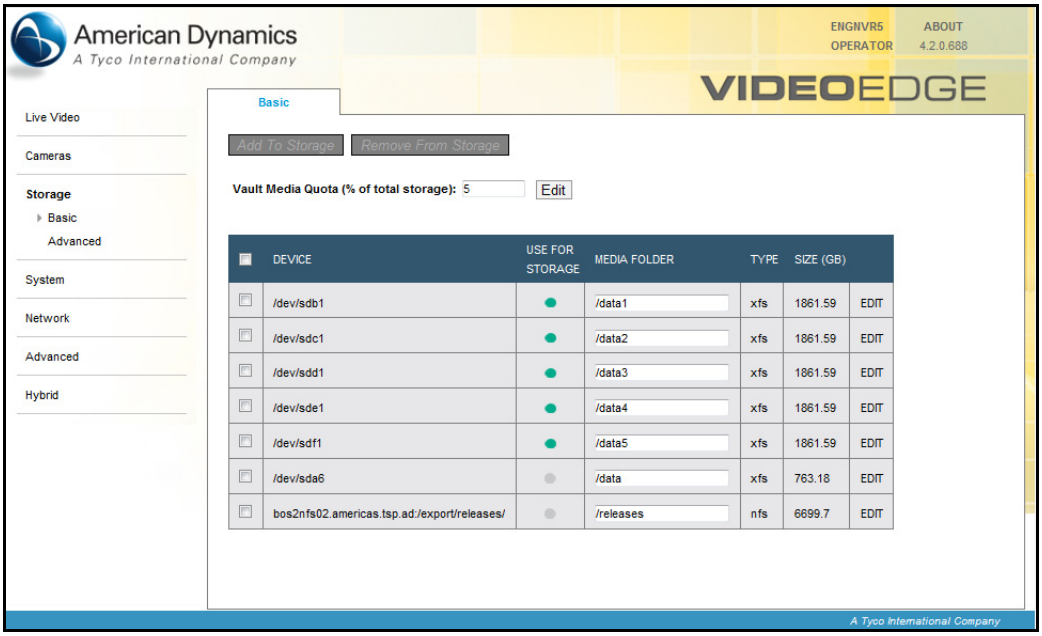



**Table 5-1 Basic Storage Configuration Fields**

| Field | Description |
|---|---|
| Device | A physical device detected by the NVR. |
| Use for Storage | Indicates whether or not the device is being used for storage.<br>Green indicator = Enabled for storage<br>Gray indicator = Disabled for storage<br>Red indicator = Media folder is unhealthy |
| Media Folder | The location on the device where recorded media will be stored. |
| Type | Indicates the file system type, for example, XFS |
| Size (GB) | The total size of the storage device in GB. |
| Amount to Use for Media | The total amount of space to be used for storing media before data culling begins on the stored media.<br><br>**Note**<br>The amount of space to be used for media cannot exceed the total size of the storage device but must meet the minimum storage requirement (10GB). |

# Enabling Media Folders for Storage

If there are devices available in the basic storage configuration table, media cannot be recorded to

these devices until the corresponding media folder(s) are enabled for storage. By default when a device is added to the NVR, the media folder is NOT enabled for storage. You must enable the media folders for storage in order to store media.

### Procedure 5-1
### Enabling a Media Folder to be Used for Storage

| Step | Action |
|---|---|
| 1 | Select the **Storage** menu. |
| 2 | Select **Basic**.<br>The Basic Storage Configuration page opens (Figure 5-1). |
| 3 | Select the checkbox for the media folder you want to use for storage and click **Add To Storage**.<br>Or<br>Select **EDIT** in the media folder record you want to use for storage, in the **Use For Storage** field select the dropdown arrow, click the **Enable** indicator then select **Save**.<br>The **Use For Storage** indicator turns green, indicating that the media folder is to be used for storage.<br>**Note**<br>If there has been media already stored in the folder a pop-up window will open asking 'Do you wish to delete all previously recorded media from this folder?'. Click **Yes** or **No** as required. |

**- End -**

## Disabling Storage Media Folders

If you need to remove a media folder from storage, you must disable it. When a media folder is removed from storage, the recorded media in the folder is not removed by default. You are given the option to retain or remove the recorded media. Information in the media database is however removed. When you remove a media folder, if the NVR is actively recording to that folder it will automatically transition recording to another media folder in the same storage set. Once a media folder is removed from storage the NVR will no longer record to that folder.

### Procedure 5-2
### Disabling a Storage Media Folder

| Step | Action |
|---|---|
| 1 | Select the **Storage** menu. |
| 2 | Select **Basic**.<br>The Basic Storage Configuration page opens (Figure 5-1). |

3 Select the checkbox for the media folder you want to use for storage and click **Remove From Storage**.

Or

Select **EDIT** in the media folder record you want to use for storage, in the **Use For Storage** field select the dropdown arrow, click the **Disable** indicator then select **Save**.

4 Click **OK** to delete any previously recorded media.

The **Use For Storage** indicator turns gray, indicating that the media folder is not being used for storage.

**- End -**

# Allocating Storage Space for Media

When a media folder has been enabled for storage, by default all of the media folder will be used for storage. You can set the amount of space to be used for storage as required.

## Procedure 5-3
## Allocating Storage Space for Media

| Step | Action |
|---|---|

1 Select the **Storage** menu.

2 Select **Basic**.

The Basic Storage Configuration page opens (Figure 5-1).

3 Select **EDIT** in the media folder record for which you want to assign storage space.

4 Enter the amount of storage space you want to reserve for media, in this folder, in the **Amount to Use For Media** field.

**Note**

1 The **Amount to Use for Media** entered cannot exceed the total size available.

2 If the storage space specified does not meet minimum storage capacity requirements (10GB), a warning message displays.

5 Click **Save**.

**- End -**

# Data Culling

When there is not enough space in a storage set to store recorded media, media will be deleted.

If there is any media older than the maximum retention period specified for a specific camera, the media will be automatically deleted.

The available space in each storage set is determined periodically. If the available space in a storage set falls below the data-culling threshold, media will be deleted for any camera in the storage set which is older than the maximum retention period. If you do not set a maximum retention period for a camera, all media for this camera may be deleted to free up storage space, as the NVR will prioritize saving the media stored for cameras up to their maximum retention period. The oldest media is deleted first, minute by minute, until the free space limit is reached. If there is no media older than the retention period, the oldest media in the storage set is deleted and an alarm is raised.

**Note**

The media deleted will only be the oldest media available online.

The alarm is an indication that there is insufficient storage space available for the media that you want to store. To resolve this issue you can add additional storage devices to the NVR, decrease the maximum retention period for camera(s) or use Advanced Storage Configuration settings to move cameras to another storage set. To add additional media storage refer to Connecting Additional Storage Devices on page 228.

# Vaulted Media

Vaulted media is specific media tagged so it will not be deleted, until specified. Vaulted media will not be deleted as part of the normal data culling process of media storage folders.

Use victor unified client to tag media as protected media using the Vault feature. You must have ‘Protect’ permissions to set video as protected media. To allow vaulted media to be deleted you must set it as unprotected using victor unified client and have ‘Unprotect’ permissions. For more information refer to the Vault chapter in the victor Configuration and User Guide.

## Vault Media Quota

A vault media quota is a percentage of the total storage available that is to be used to store vaulted media only.

Over time the amount of vaulted media within a storage set will accumulate. If too much vaulted media accumulates it may result in non vaulted media being prematurely culled when the storage space reaches its maximum capacity. A vault media quota can be set to prevent premature data culling as the amount of space for vaulted media is limited ensuring there is enough space for normal media storage.

When you are assigning media as vaulted, and if there is not enough storage space in the quota allocated to store the media as vaulted media, a warning message opens and you cannot assign the media as vaulted. You will need to increase the vault media quota or delete vaulted media.

### Procedure 5-4
### Setting a Vaulted Media Quota

| Step | Action |
|---|---|
| 1 | Select the **Storage** menu. |
| 2 | Select **Basic**. |

The Basic Storage Configuration page opens (Figure 5-1).

3 Click **Edit**.

4 Enter the required protected media quota, as a percentage of the total space available, in the **Vault Media Quota** field.

5 Click **Save.**

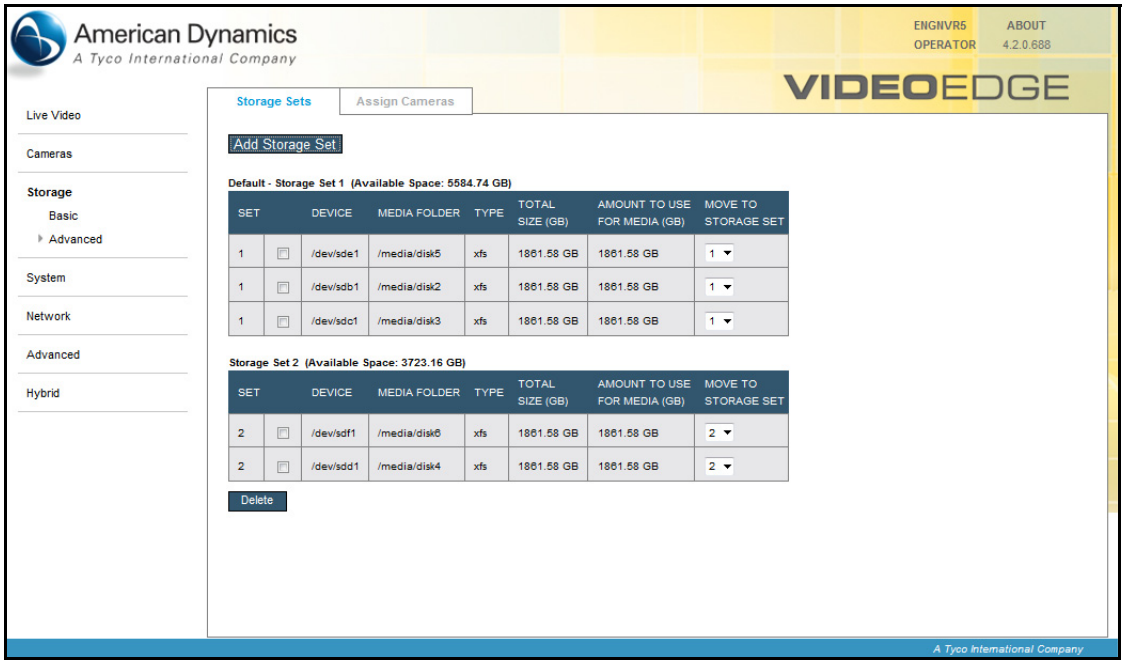
**- End -**

## Advanced Storage Configuration

The Advanced Storage Configuration options allow you to be flexible in setting up the storage on the NVR. You can spread media folders and cameras across storage sets to achieve higher system performance due to a lower total data rate required to record to each storage device.

By default there is one storage set created on the NVR. It initially contains all media devices detected by the NVR and are available to view through the Basic Storage Configuration page. Once a media folder on a storage device is enabled for storage in the Basic Storage Configuration page, the media folder is available for advanced configuration and is displayed in the Advanced Configuration page in Storage Set 1. Table 5-2 describes the fields in the Advanced Storage Configuration storage sets.

## Figure 5-2 Advanced Storage Configuration




## Table 5-2 Advanced Storage Configuration Fields

| Field | Description |
|---|---|
| Set | This is the Storage Set the media folder is assigned to. |
| Device | This is a physical device detected by the NVR. |
| Media Folder | The location on the device where recorded media will be stored. |
| Type | Indicates the file system type, for example, XFS |
| Total Size (GB) | The total size of the storage device in GB. |
| Amount to Use for Media (GB) | The total amount of space to be used for storing media before the stored media begins to data cull.<br><br>**Note**<br>The amount of space to be used for media cannot exceed the total size of the storage device. |
| Move to Storage Set | A dropdown list of other storage sets available on the NVR. By selecting a storage set you will move the media folder to that storage set. |

Using the Advanced Storage Configuration page you can:

- Create storage sets
- Delete storage sets
- Add media folders to storage sets
- Move media folders between storage sets

- Assign cameras to storage sets
- Move cameras between storage sets
- Calibrate cameras

By using a combination of the advanced configuration options and your calculated storage requirements per camera, you can configure the NVR to achieve optimal efficiency and performance.

# Creating Storage Sets

You can create a new storage set to group particular media folders and cameras. When a new storage set is created it contains no media folders or cameras, you need to reassign these from another storage set.

## Storage Set Recommendations

- If you are using RAID storage systems, American Dynamics strongly recommends assigning all virtual disks from a disk group to the same storage set.
- It is recommended that a storage set should contain a minimal number of media folders, one if possible, maximizing the virtual disk size.
- The R710 bundled server storage set performance supports a maximum of 32 cameras or 100Mbps on each storage set, whichever is reached first. Total input to server is 400Mbps.
- The R720 bundled server storage set performance supports a maximum of 64 cameras or 200Mbps on each storage set, whichever is reached first. Total input to server is 400Mbps.
- The Software Only option, installed on hardware that meets the minimum requirements, supports a maximum of 32 cameras or 100Mbps on each storage set, whichever is reached first. Total input to server is 400Mbps.

### Procedure 5-5
### Creating a Storage Set

| Step | Action |
|---|---|
| 1 | Select the **Storage** menu. |
| 2 | Select **Advanced**.<br>The Advanced Storage Configuration page opens (Figure 5-2). |
| 3 | Click **Add Storage Set**.<br>A new storage set is created. |

**- End -**

# Media Folder Assignment for Storage Sets

When you create a new storage set you need to assign media folders and cameras to it. To assign media folders to a new storage set you need to reassign media folders from the default storage set or an existing storage set.

There is no limit to the number of media folders you can assign to a storage set. There are however some restrictions:

- You are able to add a system disk to a storage set by specifying a particular folder on the system disk. It is recommended that the folder you specify exists on a separate partition on the system disk.
- You will not be presented with Linux system file systems, for example, /proc, /sys, etc.

**Note**

When allocating media folders from the same device or RAID group it is recommended to associate them with the same storage set. Hard drive thrashing can occur if media folders from the same hard drive are spread across several storage sets, this could result in the systems performance being downgraded when the hard drive is being overworked.

When a media folder is moved to another storage set, all previously recorded media will still be retrievable via clip export and playback in victor unified client.

### Procedure 5-6
### Assigning / Reassigning Media Folders to a Storage Set

| Step | Action |
|---|---|
| **1** | Select **Storage** from the main menu. |
| **2** | Select **Advanced**.<br>The Advanced Storage Configuration page opens (Figure 5-2). |
| **3** | Locate the media folder in its existing storage set that you want to move to a new storage set. |
| **4** | Select the new storage set you want to assign the media folder to, from the **Move to Storage Set** dropdown list.<br>The media folder is reassigned to the new storage set. |

**- End -**

# Assigning Cameras to Storage Sets

During the process of adding cameras to the NVR, if only the default storage set is available, the new camera will be added to this storage set. However, if there are a number of storage sets available you will be prompted to assign the camera to the required storage set. Cameras can be reassigned to different storage sets as required without needing to remove and re-add the camera. If you are adding cameras using auto-discovery the cameras will be added to the default storage set.

## Procedure 5-7
## Reassigning a Camera to a Different Storage Set

| Step | Action |
|---|---|

1 Select **Storage** from the main menu.

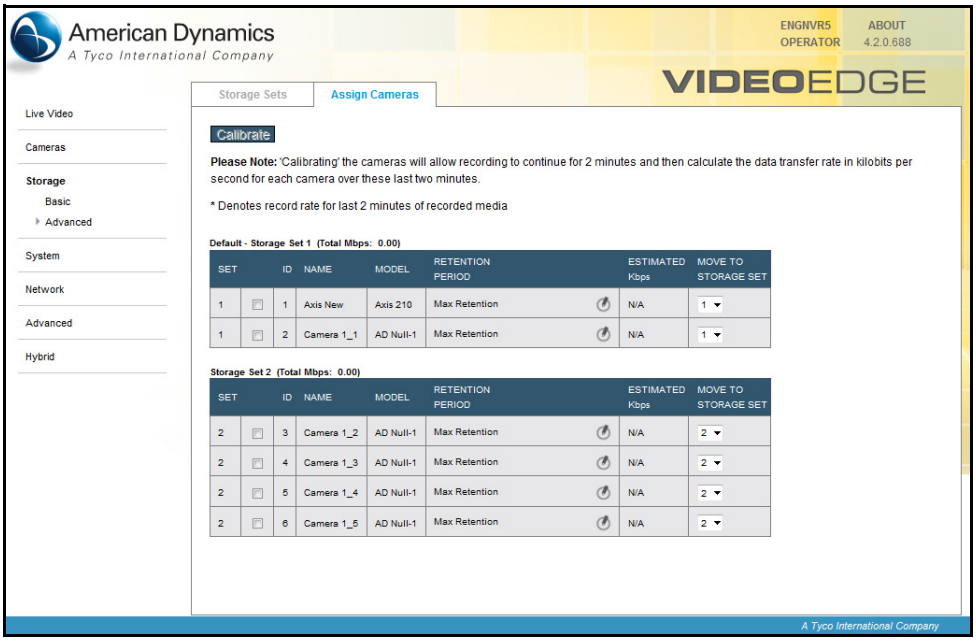
2 Select **Advanced**.

The Advanced Storage Configuration page opens (Figure 5-2).

3 Select the **Assign Cameras** tab.

A summary of cameras assigned to storage sets are displayed.

**Figure 5-3 Assign Cameras Tab**


American Dynamics
A Tyco International Company
ENGNVR5
OPERATOR
ABOUT
4.2.0.688
VIDEOEDGE
Storage Sets
Assign Cameras
Live Video
Cameras
Storage
Basic
Advanced
System
Network
Advanced
Hybrid
Calibrate
Please Note: 'Calibrating' the cameras will allow recording to continue for 2 minutes and then calculate the data transfer rate in kilobits per second for each camera over these last two minutes.
* Denotes record rate for last 2 minutes of recorded media
Default - Storage Set 1 (Total Mbps: 0.00)
SET ID NAME MODEL RETENTION PERIOD ESTIMATED Kbps MOVE TO STORAGE SET
1 1 Axis New Axis 210 Max Retention N/A 1
1 2 Camera 1_1 AD Null-1 Max Retention N/A 1
Storage Set 2 (Total Mbps: 0.00)
SET ID NAME MODEL RETENTION PERIOD ESTIMATED Kbps MOVE TO STORAGE SET
2 3 Camera 1_2 AD Null-1 Max Retention N/A 2
2 4 Camera 1_3 AD Null-1 Max Retention N/A 2
2 5 Camera 1_4 AD Null-1 Max Retention N/A 2
2 6 Camera 1_5 AD Null-1 Max Retention N/A 2
A Tyco International Company

4 Locate the camera you want to reassign in its existing storage set.

5 Select the storage set you want to reassign the camera to from the **Move to Storage Set** dropdown list.

The camera is reassigned to the selected storage set.

**- End -**

# Calibrating Cameras

The data transfer rate for a camera is displayed in each storage set table. This is recorded in the **Estimated Kbps** field. The data transfer rate displayed in this field usually displays the average rate over the last 24 hour period in kbps. You can use the Calibrate camera function to calculate the data transfer rate in kbps for each camera over the last two minutes. This will give an up to date data transfer rate for each camera. You can use this information to optimize the performance of your NVR by reassigning cameras to storage sets based on the current data transfer rates.

### Procedure 5-8
### Calibrating Cameras

| Step | Action |
|---|---|
| 1 | Select **Storage** from the main menu. |
| 2 | Select **Advanced**.<br>The Advanced Storage Configuration page opens (Figure 5-2). |
| 3 | Select the **Assign Cameras** tab.<br>A summary of cameras assigned to storage sets are displayed. |
| 4 | Click **Calibrate**.<br>The **Estimated Kbps** field for each camera is updated with the data transfer rate for the last two minutes. |

**- End -**

## Deleting Storage Sets

You can delete storage sets as required, however, the default storage set cannot be deleted.

**Note**

Before you delete a storage set you need to ensure that it contains no assigned cameras or media folders.

### Procedure 5-9
### Deleting a Storage Set

| Step | Action |
|---|---|
| 1 | Select **Storage** from the main menu. |
| 2 | Select **Advanced**.<br>The Advanced Storage Configuration page opens (Figure 5-2). |
| 3 | Reassign all media folders currently assigned to the storage set you want to delete, see Procedure 5-6 Assigning / Reassigning Media Folders to a Storage Set on page 68 for further information. |
| 4 | Reassign all cameras currently assigned to the storage set you want to delete, see Procedure 5-7 Reassigning a Camera to a Different Storage Set on page 69 for further information. |

5 Click the **Delete** button under the storage set you want to delete.

**Note**

If you have not reassigned all cameras and media folders the NVR will not allow you to delete the storage set.

**- End -**

## Storage Statistics

The NVR holds and displays storage statistics for storage devices, storage sets and cameras that are being used in the NVR storage configuration. These can be accessed via the Advanced menu. Refer to Storage Statistics on page 194 for further information.

## Storage Monitoring

All media folders assigned to a storage set will be monitored by the NVR to determine that they are operational and available for storing media.

The media folders are checked to ensure they are still mounted and read/writable. It is possible that media folders can become unmounted due to system errors, device errors or the device being unmounted by a user. A media folder could become read-only, for example, if the device has been unmounted and remounted as read-only.

If a media folder is determined as non-operational, recording will switch to the next available operational media folder in the storage set.

Non-operational media folders are highlighted as being unhealthy.

To determine the health status of storage devices, view the Status in the Device section of the Storage Statistics page.

# Live Video

## Overview

Once the NVR system has been configured you can view live video streams.

**Note**

If you are accessing the NVR using the victor client NVR configuration page, you can not view live video. Use the Surveillance tab in your victor client.

## Viewing Live Video

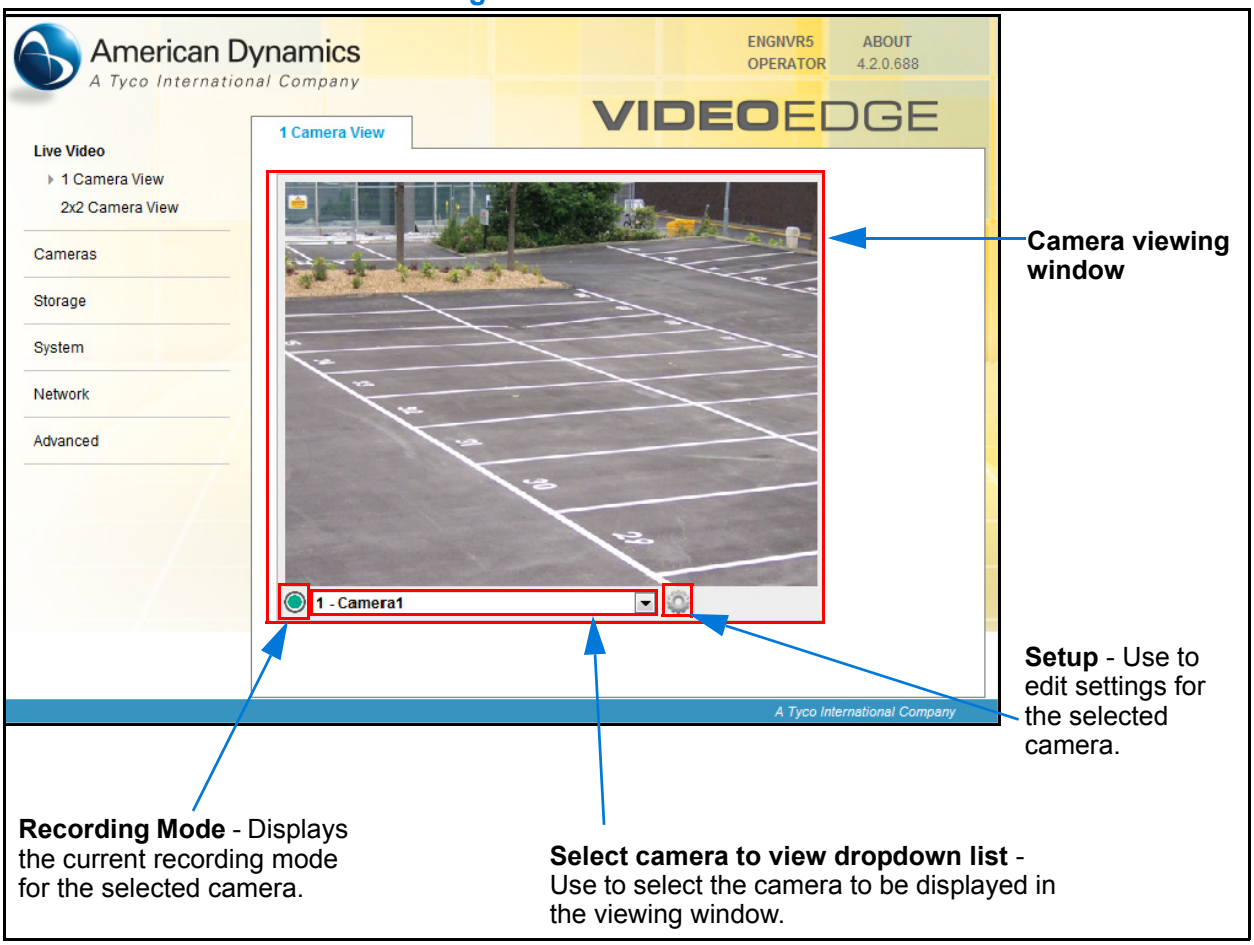
The camera views on an NVR can display live video up to a maximum of 4 live video streams. A live audio stream is not available on the NVR Configuration interface. To listen to audio use victor unified client.

Viewing Live Video on the NVR Web Interface uses Apple QuickTime, you must have the QuickTime player installed to be able to view video. This allows you to view video within the web interface and as stand alone QuickTime windows.

You can download it from www.apple.com/quicktime. If you try to view Live Video and do not have QuickTime installed you will be notified that a plugin is required. Selecting to Install the plugin will direct you to the Apple website.

You must have your storage and cameras configured before you can view live video.

## Figure 6-1 Live Video View




## Procedure 6-1
## Viewing Live Video

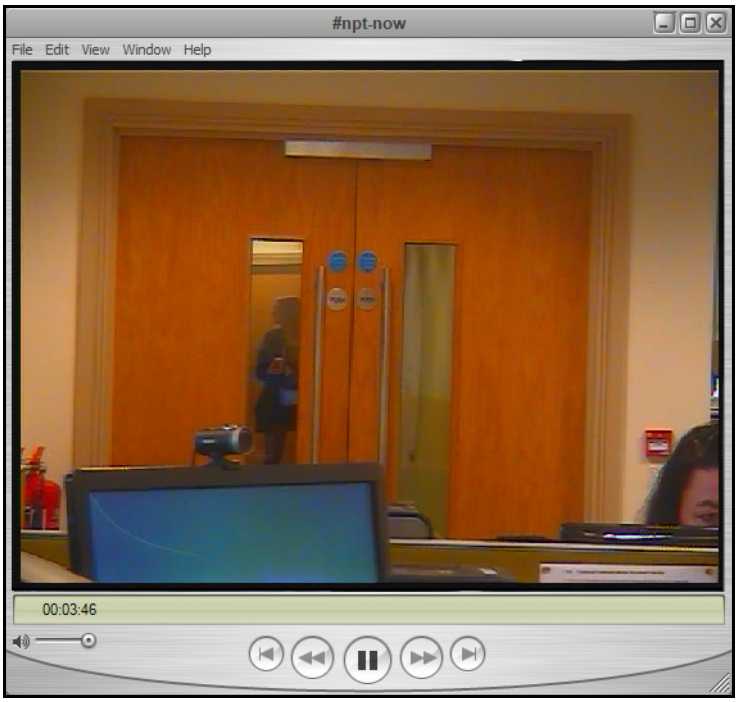
| Step | Action |
|---|---|
| 1 | Select **Live Video** from the main menu. |
| 2 | Select **1 Camera View**<br>Or<br>Select **2x2 Camera View**. |
| 3 | Select the camera(s) you want to view from the **Select camera to view** dropdown list.<br>The camera's live video stream displays in the viewing window. |

**- End -**

# Viewing Live Video with QuickTime

You can click on the viewing area of a camera to open a QuickTime viewer showing that camera's video stream (Figure 6-2).

**Figure 6-2 QuickTime Viewer**




## Procedure 6-2
## Opening a QuickTime Viewer for a Camera

| Step | Action |
|---|---|
| 1 | From any camera live view, click in the camera viewing window.<br>A QuickTime Internet Authorization dialog box opens. |
| 2 | Enter your **User ID.** |
| 3 | Enter your **Password.** |
| 4 | Click **OK**.<br>The QuickTime viewer. |

**- End -**

# Camera List

## Overview

The Camera List displays a list of all cameras added to the NVR. The Camera List summary table (Table 7-1) gives a summary of all camera configuration settings that are available to view and edit in the Camera List page. You can add cameras to the NVR, remove cameras and edit camera settings from the Camera List. If you want multiple cameras to have the same configuration settings, you can batch edit numerous cameras and all assigned settings will be the same for all selected cameras provided the camera has the ability to support the selected settings.

**Figure 7-1 Camera List**

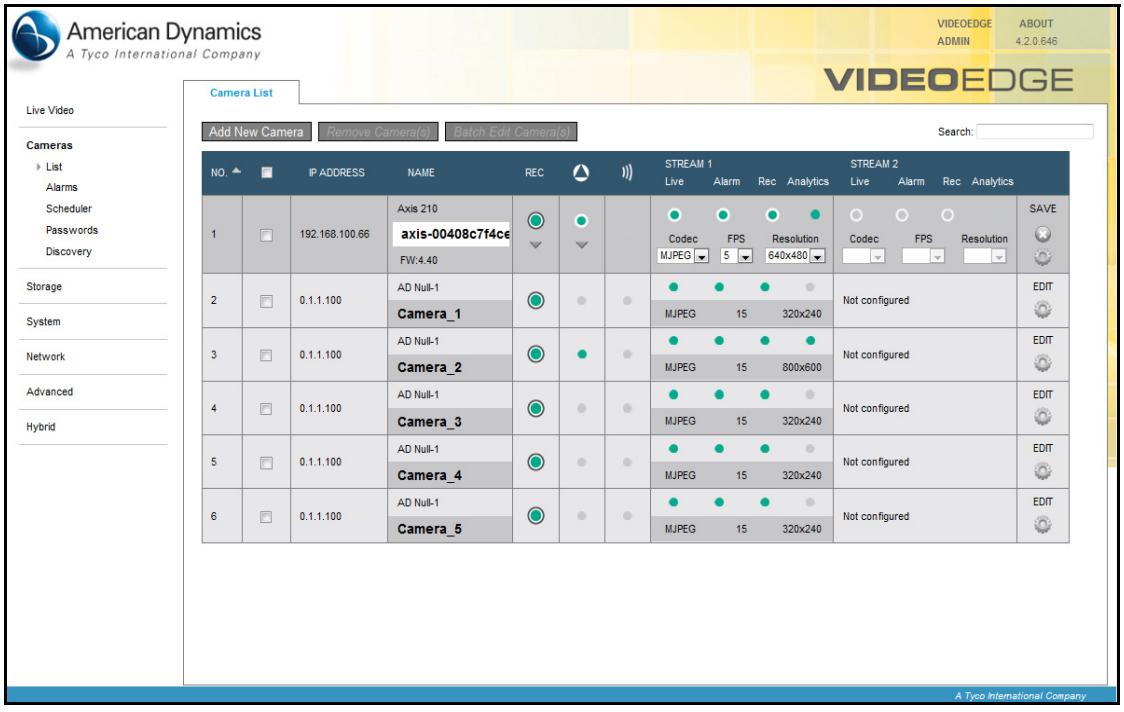



**Table 7-1 Camera List Summary**

| Field | Description |
|---|---|
| No | Camera slot number. |
| IP Address | Camera IP address |

| Field | | Description |
|---|---|---|
| Name | | Camera name as given when adding the camera to the NVR. |
| Rec | | Displays the camera recording state. There are four available options to select:<br>• Recording Off<br>• Recording Always<br>• Recording Normal Off, Alarm On<br>• Recording Always With Alarm On<br>If the scheduler is enabled, you cannot change the camera recording state and the icon, is displayed in the field. |
| Analytics | | Indicates if analytics are set on the camera.<br>There are three analytic options:<br>• Analytics Off<br>• Motion Detection<br>• Video Intelligence (This encompasses object detection, direction, linger, enter, exit and abandoned/removed) |
| Audio | | Indicates if audio is enabled or disabled on the camera. The indicator is green when audio is enabled. |
| Stream 1 / Stream 2 | Live | Indicates that this stream will be used for live streaming. |
| | Alarm | Indicates that this stream will be used for any alarms that are recorded. |
| | Rec | Indicates that this stream will be used for non-alarm recording. |
| | Analytics | Indicates that this stream will be used for executing analytics (motion detection or video intelligence).<br>**Note**<br>If an alarm is raised for motion detection or video intelligence, the alarm stream is used to record the alarm. |
| | Codec | The camera codec. |
| | FPS | The camera FPS. |
| | Resolution | The camera resolution. |

# Viewing the Camera List

By viewing the camera list you can view a snapshot of all camera's, and their basic settings, that are available on the NVR.

### Procedure 7-1
### Viewing the Camera List

| Step | Action |
|---|---|
| 1 | Select the **Cameras** menu. |
| 2 | Select **List**.<br>The Camera List opens (Figure 7-1) displaying a table of all cameras currently connected to the NVR. |

**- End -**

# Sorting the Camera List

The Camera List can be sorted alphanumerically by a selected column in ascending or descending order.

### Procedure 7-2
### Sorting the Camera List

| Step | Action |
|---|---|
| 1 | Select the **Cameras** menu. |
| 2 | Select **List**.<br>The Camera List opens (Figure 7-1). |
| 3 | Select the column header from the Camera List table that you want to sort by.<br>The list is sorted in alphanumeric order. |
| 4 | Sort in ascending or descending order:<br>**a** Select to sort in ascending order.<br>**b** Select to sort in descending order. |

**- End -**

# Filtering the Camera List

The Camera List has a Filter feature which can be used to display specific camera records. The filter feature will look at the criteria entered and compare this against all fields in the camera list.

For example, if you enter criteria that matches characters in a camera name, all cameras will be displayed that match the given filter criteria in their name. This feature can be useful when looking for a particular camera in a large list of cameras.

### Procedure 7-3
### Filtering the Camera List

| Step | Action |
|---|---|
| 1 | Select the **Cameras** menu. |
| 2 | Select **List**.<br>The Camera List opens (Figure 7-1). |
| 3 | Enter the filter criteria into the **Filter** field.<br>The Camera List table filters, displaying only cameras that meet the criteria entered.<br>**Note**<br>The Camera List will filter as you type the criteria into the **Filter** field. As the criteria gets more specific the list filters correspondingly. |

**- End -**

## Manually Adding an IP Camera or Encoder

The procedure for manually adding an IP camera or encoder to the NVR is generally consistent across different camera types.

**Note**

The easiest method of adding cameras to the NVR is by using the Camera Auto-Discovery feature. However, you can also manually add cameras if required. For further information about Camera Auto-Discovery, see Adding Cameras Using Auto-Discovery on page 82.

When a camera is manually added to the NVR the default recording mode is set to Recording Always. If the configuration of the camera does not support Motion Detection (using either a primary or secondary stream) then the default recording mode will be Record Always.

When you add an encoder to the NVR, all cameras associated with this encoder will have the same IP address. As a result, these cameras must be assigned to the same password group and have the same dry contact settings. If you edit either the password group or the dry contact settings for one camera associated with the encoder, these settings will be updated for all cameras.

## Procedure 7-4
## Manually Adding an IP Camera or Encoder

| Step | Action |
|---|---|

1 Select the **Cameras** menu.

2 Select **List**.

The Camera List opens (Figure 7-1).

3 Click **Add New Camera**.

**Figure 7-2 Add New Camera Window**

4 Enter the **Camera Name**.

5 Enter the **Internal IP Address** of the camera.

6 Select the **Password Group** of the camera from the dropdown list.

**Note**

The **Password Group** will usually be default. The NVR will use the manufacturer's default password to connect to the camera. However, if you have changed the password for this camera, you need to assign the camera to the appropriate password group, or create a new password group. For further information on password groups refer to Camera Password Groups on page 131.

7 (Optional) Select the **Storage Set** from the dropdown list.

**Note**

1 This option is only available if you are using advanced storage configuration.The **Storage Set** dropdown list displays all storage sets with at least one storage media folder assigned. The selected storage set is where the camera will record to.

2 If you are using basic storage configuration, the camera will automatically be assigned to the default storage set.

8 Click **Apply**.

The camera is added to the Camera List.

9 Configure the camera settings as required.

**- End -**

## Adding Cameras Using Auto-Discovery

The camera Auto-Discovery feature allows you to automatically discover cameras on the network to add to the NVR. When the cameras are discovered you can add as many cameras until you reach your limit of camera licences. The default recording status for cameras added via auto-discovery is Record Always.

**Note**

When using camera Auto-Discovery, it is recommended that the camera network you are using to discover cameras on, has a Subnet Mask of 255.255.255.0.

Not all cameras can be added to the NVR in this way as some manufacturers require cameras to be pre-configured prior to being added to a network.

To avoid problems with auto-discovery:

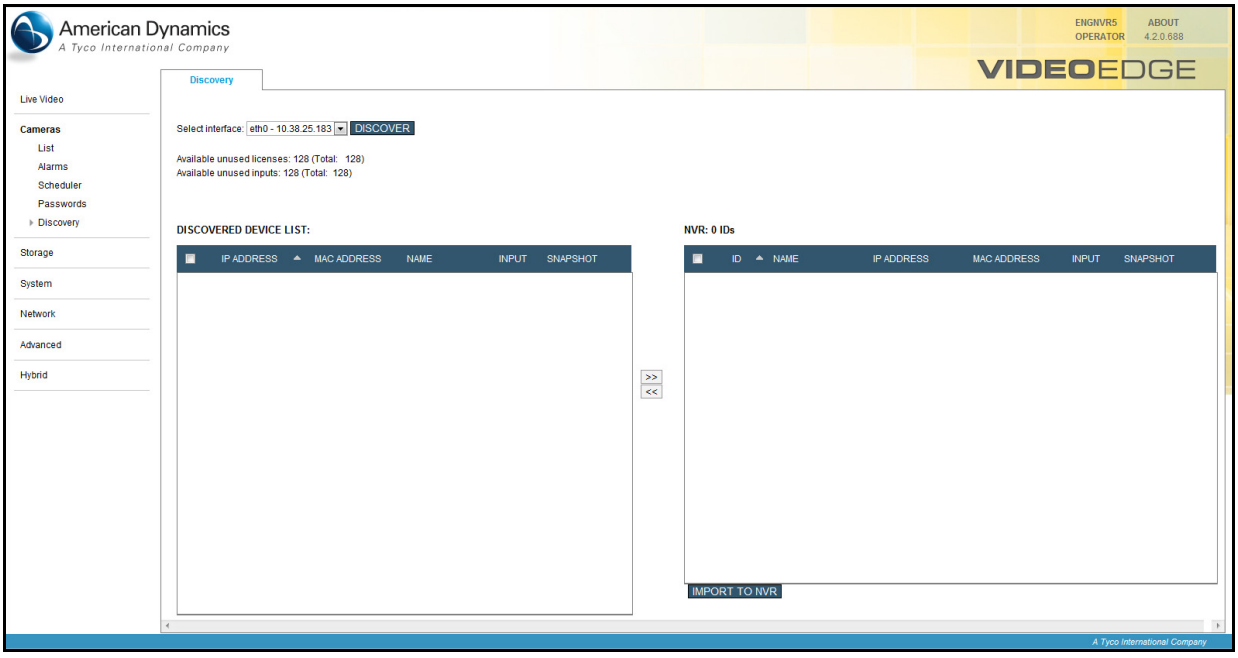
1 Make sure the NVR is on the network and is online.

2 Connect the network cameras to the NVR.

3 Power on the network cameras. After the cameras have finished their initialization you can use the auto-discovery feature.

4 Ensure the IP cameras are using the manufacturer's default username and password.

Figure 7-3 Camera Auto-Discovery




## Procedure 7-5
## Adding Cameras using Auto-Discovery

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Discovery**.<br>The Camera Auto-Discovery page opens (Figure 7-3). |
| 3 | Select the network from the **Select interface** dropdown list that you want to discover cameras on. |
| 4 | Click **Discover**.<br>The Auto-Discovery feature searches for cameras on the network which may take a few minutes. Cameras that are discovered are displayed in the Discovered Device List.<br>**Note**<br>If there are cameras that you expected to be discovered, but are not displayed, you may need to add these cameras manually as some manufacturers require cameras to be pre-configured. |
| 5 | Select the checkbox(es) for the camera(s) you want to add to the NVR from the Discovered Device List. |
| 6 | Use the arrow right button [>>] to move the selected cameras to the NVR list. |
| 7 | Select the checkbox(es) of the camera(s) you want to import to the NVR from the NVR list. |
| 8 | Click **Import to NVR**.<br>The selected camera(s) are imported into the NVR Cameras List. |
| 9 | Select **List** from the **Cameras** sub-menu. |

The imported camera(s) are displayed in the Camera List.

**- End -**

# Removing a Camera

You can remove a camera from the NVR if necessary. Once you remove a camera from the NVR, you will no longer be able to view live video, record media or access the camera via victor unified client.

## Procedure 7-6
## Removing a Camera

| Step | Action |
|---|---|

**1** Select **Cameras** from the main menu.

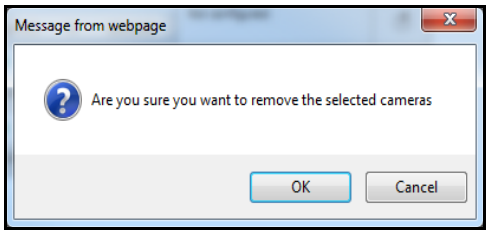
**2** Select **List**.

The Camera List opens (Figure 7-1).

**3** Select the checkbox in the camera record(s) of the camera(s) you want to remove.

**4** Click **Remove Camera(s)**.

A message box opens for confirmation that you want to remove the camera(s).




**5** Click **OK**.

**6** The camera(s) are removed from the NVR.

**- End -**

# Camera Configuration

## Overview

This chapter describes how to configure cameras that have been added to the NVR. You can configure one camera on its own, or if required, you can configure multiple cameras together with the same settings, using batch camera configuration.

To configure camera settings, use the Camera List page. If you use the Camera List summary table you can edit basic camera settings, however if you click the Setup icon for a particular camera additional tabs open. From these tabs you can configure all the supported settings for a selected camera.

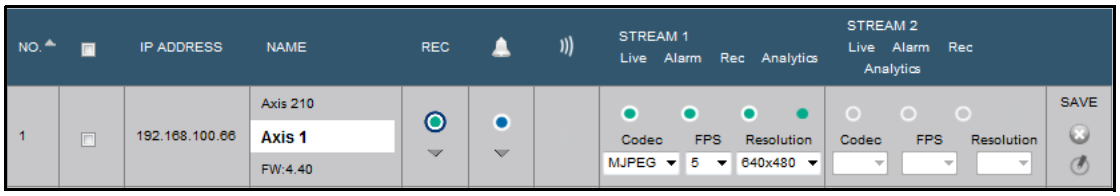
## Basic Camera Configuration

The settings displayed for each camera in the Camera List are a summary of the current camera configuration settings. All camera settings can be updated using advanced camera configuration, refer to Advanced Camera Configuration on page 89. However, basic camera settings displayed in the Camera List can be edited within the Camera List page. These include, editing the camera name, updating the recording mode, enabling or disabling Motion Detection or Video Intelligence, enabling/disabling audio and configuring most stream configuration settings.

### Procedure 8-1
### Editing Basic Camera Settings via the Camera List

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**.<br>The Camera List opens (Figure 8-1). |
| 3 | Select **Edit** in the camera record for which you want to edit a camera list setting.<br>The fields that you can update are ready to edit. |

**Figure 8-1 Camera List Fields**




**4** Make the required changes to:

- **Name** - Use this field to update the name of the camera.
- **Rec** - Use this to update the camera recording state. You can choose, Recording Off, Recording Always, Recording Normal Off, Alarm On, or Recording Always With Alarm On. For more information refer to Recording Statuses on page 95.

**Note**

To update a camera's recording state you must ensure the camera recording scheduler is disabled.

- **Analytics** - Use this to change the analytic alarm setting. You can select, Analytics Off, Motion Detection or Video Intelligence.
- **Stream 1 / Stream 2** settings. If a second stream is available on the camera, use these settings to select which stream is to be used for:

**a** Live video,

**b** Alarms, and

**c** Recording.

You can assign each of these to either Stream 1 or Stream 2 as required.

You can also adjust the **Codec**, **FPS** and stream **Resolution** settings for each stream.

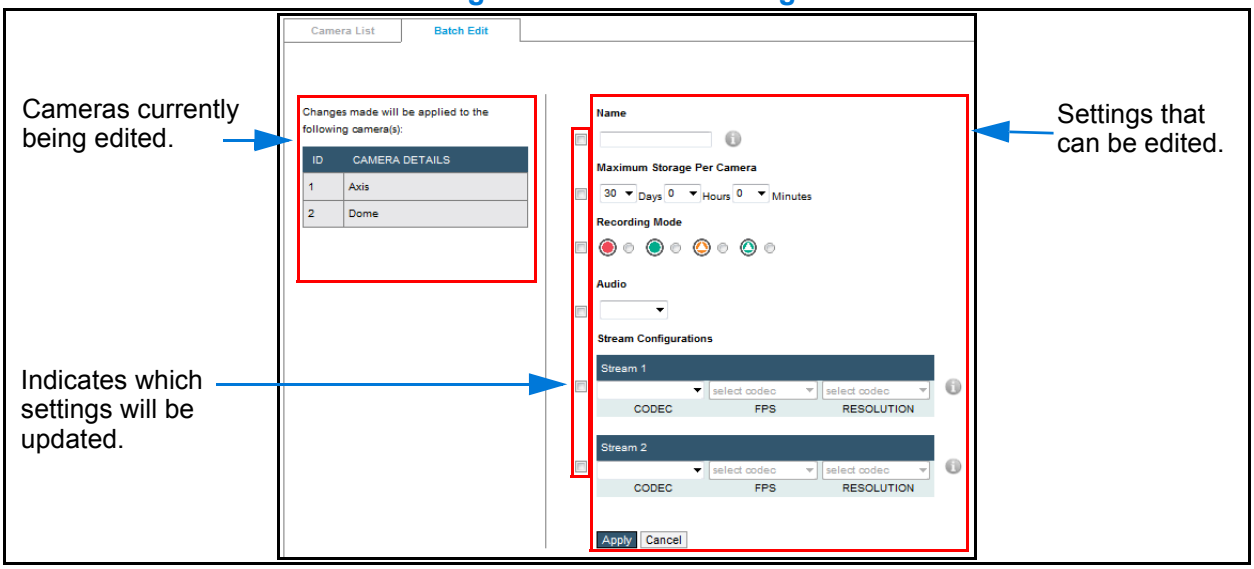
**5** Click **Save**.

**- End -**

# Batch Camera Configuration

Some camera settings can be edited in batch. The Batch Edit page (Figure 8-2) lists the cameras currently being edited in the left pane, and the setting adjustments are made in the pane on the right. When a change is made to a setting, the checkbox next to the setting is checked. When you deselect the checkbox, the new setting adjustment will not be applied to the cameras. Before you apply the setting adjustments to all cameras, the changes that will be made to the settings are previewed, with the new settings highlighted in yellow.

**Figure 8-2 Batch Edit Page**




## Procedure 8-2
## Batch Editing Camera Settings

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Select the checkbox for each camera you want to edit in batch.

4 Click **Batch Edit Camera(s)**.

The Batch Edit page opens (Figure 8-2).

5 Adjust the camera settings:

**a** **Name** - Use this field to update the name of the cameras.

**Note**

When you update the name of cameras using batch edit, each camera will have a number appended to its name. For example, **CameraName_1**, **CameraName_2**, etc.

**b** **Maximum Storage Per Camera** - Select from the dropdown lists to set the maximum duration over which video recorded for these cameras will be saved without being deleted.

**c** **Storage Set** - Select from the dropdown list which storage set the batch of cameras will record to.

**d** **Recording Mode** - Use this to set the recording mode for these cameras. You can set **Recording Off**, **Recording Always**, **Recording Normal Off, Alarm On** or **Recording Always with Alarm On**. Refer to Recording Statuses on page 95 for more information.

**e** **Analytics** - Select from the dropdown list which type of analytics to apply to this batch of cameras. Refer to Video Intelligence on page 113 and Motion Detection on page 103 for more information.

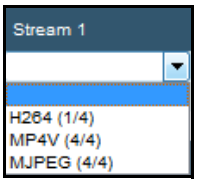
f **Audio** - Select Enabled/Disabled from the dropdown list to enable/disable audio.

g **Stream Record Modes** - Set each stream to **Live**, **Alarm** or **Record**.

h **Stream Configurations** - Set the stream configurations for **Codec**, **FPS**, **Resolution** and **Quality** in the respective dropdown fields.

**Note**

When you are selecting a value for the **Codec**, **FPS**, **Resolution** and **Quality** fields, each dropdown list contains the available options followed by a number in brackets. The number in brackets represents the number of cameras that support the value out of the total number of cameras being edited. If a codec has not been selected the dropdown list will display options supported on all codecs. It is important to note that if this is the case some options may fail on some cameras.

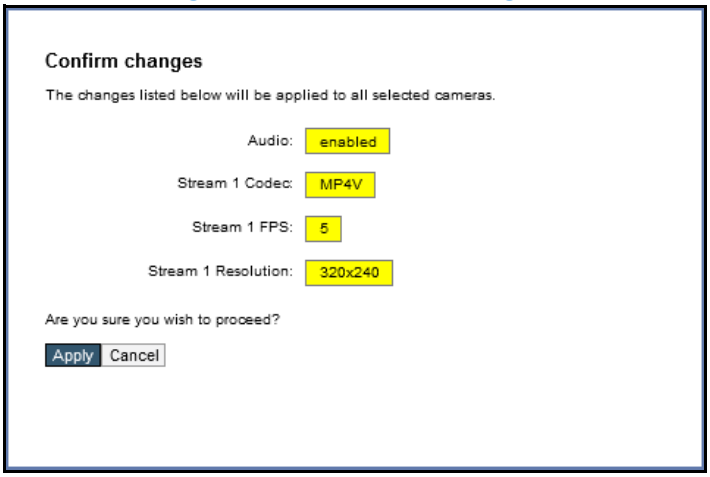



For example, Codec: MJPEG (4/4), indicates that 4 out of the 4 cameras being updated supports the Codec MJPEG.

6 Click **Apply**.

7 A Confirm Changes window opens with a preview of the changes to be made to the selected cameras.

**Figure 8-3 Confirm Changes**


Confirm changes
The changes listed below will be applied to all selected cameras.
Audio: enabled
Stream 1 Codec: MP4V
Stream 1 FPS: 5
Stream 1 Resolution: 320x240
Are you sure you wish to proceed?
Apply
Cancel

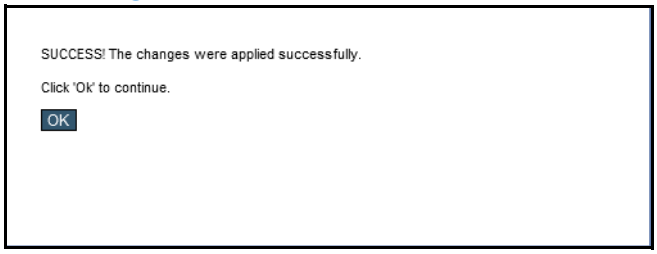
8 Click **Apply**.

**Note**

If you do not want to make these changes to all cameras, click **Cancel** and update the settings as required.

9 A message box opens to confirm the changes were successful. Click **OK**.

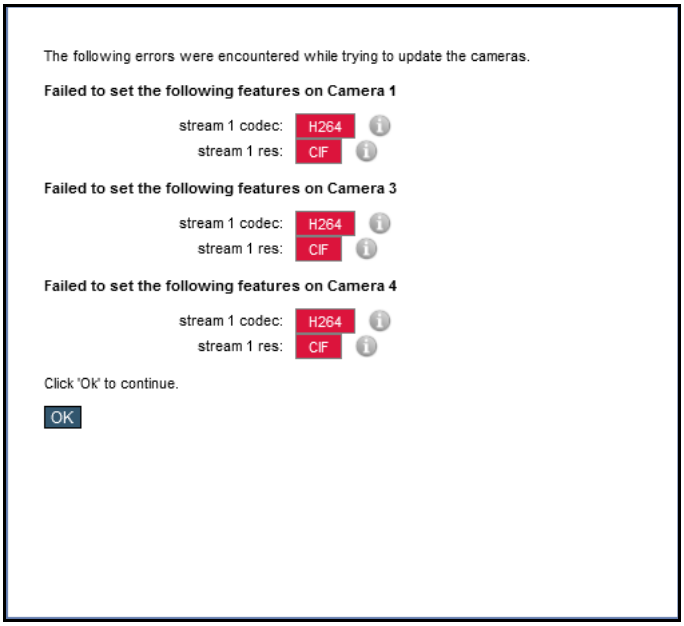
**Figure 8-4 Successful Batch Edit**




**Note**

If some of the changes are not successful, a summary page of failed updates opens with the failures highlighted in red. By hovering over you can view more detailed error information. Click **OK** to continue.

**Figure 8-5 Failed Fields in Batch Edit**


The following errors were encountered while trying to update the cameras.
Failed to set the following features on Camera 1
stream 1 codec: H264
stream 1 res: CIF
Failed to set the following features on Camera 3
stream 1 codec: H264
stream 1 res: CIF
Failed to set the following features on Camera 4
stream 1 codec: H264
stream 1 res: CIF
Click 'Ok' to continue.
OK

**- End -**

# Advanced Camera Configuration

There are several camera configuration tabs;

- General
- Image Settings
- Function and Stream
- Alerts
- PTZ

These tabs can be accessed by clicking the Setup icon in the Camera List page.

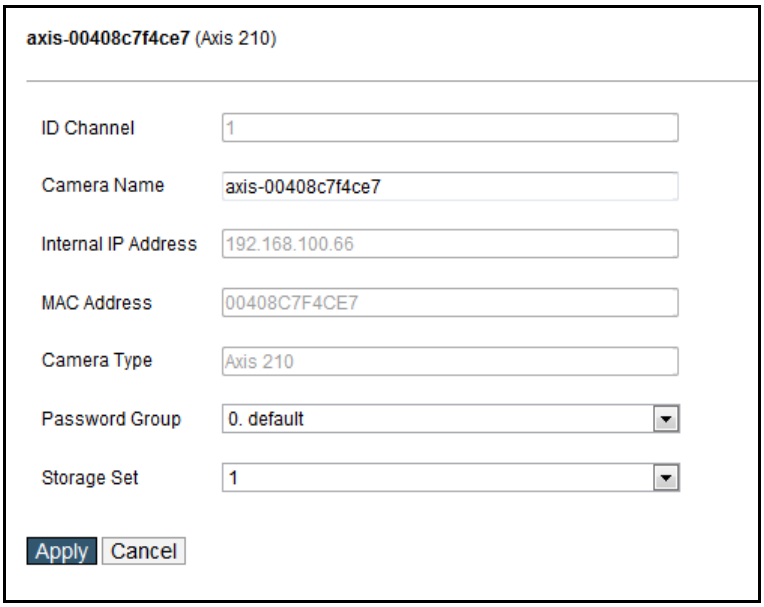
Each category is described in detail in the following sections of this chapter.

## Configuring General Camera Settings

General camera settings that can be easily updated as required. These include the camera name, password group and storage set.

The ID Channel, Internal IP Address, MAC Address and Camera Type fields are for information only and are not configurable.

**Figure 8-6 General Configuration Settings**




### Edit a Camera Name

You can update the name given to a camera as required.

### Procedure 8-3
### Editing a Camera Name

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click **Edit** in the camera record where you want to change the camera name, select the **Name** field and enter the new camera name.<br>Or<br>Click the **Setup** button in the camera record where you want to change the camera name, select the **General** tab and enter the new camera name into the **Camera Name** field. |

4 Click **Apply**.

**- End -**

## Change the Password Group Assigned to an IP Camera

If an IP camera is assigned to a password group and you have changed the password for this camera, you will need to select the new password group the camera belongs to.

### Procedure 8-4
### Changing the Password Group Assigned to an IP Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click the **Setup** button in the camera record that you want to assign to a new password group.<br>The Function & Streams page opens. |
| 4 | Select the **General** tab. |
| 5 | Select the new password group from the **Password Group** dropdown list. |
| 6 | Click **Apply**. |

**Note**

If you are editing the password group for a camera, forming part of an encoder device, all cameras related to this device will be updated with the new password group. In this instance, a warning message opens informing you that multiple cameras will be updated.

**- End -**

## Change a Camera's Storage Set

Changing the storage set a camera is assigned to is only applicable if you have configured the NVR for advanced storage. When you change the storage set, media from the camera will now be stored on media folders in the new storage set. You can also edit the storage set a camera is assigned to by editing the advanced storage settings, refer to Advanced Camera Configuration on page 89.

### Procedure 8-5
### Changing a Camera's Storage Set

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |

3 Click the **Setup** button in the camera record that you want to assign to a new storage set.

The Function & Streams page opens.

4 Select the **General** tab.

5 Select the new storage set from the **Storage Set** dropdown list.

6 Click **Apply**.

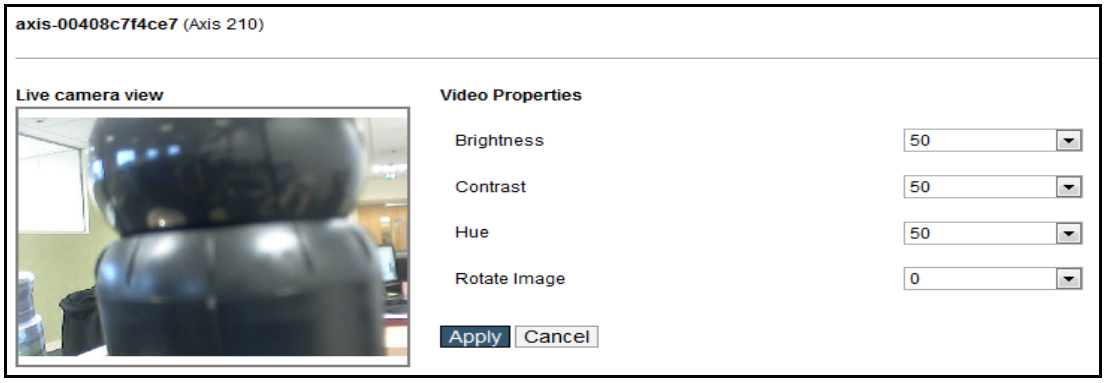
**- End -**

## Configure Camera Image Settings

Use the Image Settings options to adjust the camera image settings. The settings available are dependant on the camera make/model. When the changed settings are applied, the viewer window updates to reflect the changes made.

The settings in Figure 8-7 are an example of camera image settings.

**Figure 8-7 Image Settings**




### Procedure 8-6
### Configuring Camera Image Settings

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Click **Setup** in the camera record for which you want to configure camera settings.

The Function & Streams page opens.

4 Select the **Image Settings** tab.

5 Adjust the Video Processing Amp image settings. The available settings and value ranges are dependent on the camera make/model. The Video Processing Amp image settings include:

- **a** **Video Standard** - Select the required video processing standard from the dropdown list.
- **b** **Rotate Image** - Select the angle you want to rotate the image from the dropdown list.

c **Brightness** - Select the brightness value from the dropdown list.

d **Contrast** - Select the contrast value from the dropdown list.

e **Hue** - Select the hue value from the dropdown list.

f **Sharpness** - Select the sharpness value from the dropdown list.

g **White Balance** - Select the white balance control value from the dropdown list.

h **Back Light Compensation** - Select the back light compensation value from the dropdown list.

i **Image Interlaced** - Select the image interlacing setting from the dropdown list.

6 Adjust the Lens/Sensor settings. The types of settings and value ranges available are camera make/model dependent. The Lens/Sensor settings include:

a **Lens Focus** - Select a focus for the camera from the dropdown list.

b **Lens Auto Focus** - Select the checkbox to enable automatic camera focus.

c **Lens Iris** - Select the iris value for the camera from the dropdown list.

d **Lens Auto Iris** - Select the checkbox to enable automatic iris control.

e **Lens Day Night Mode** - Select the required mode from the dropdown list.

f **Lens WDR (Wide Dynamic Range)** - Select the checkbox to enable WDR.

7 Click **Apply**.

The viewer window updates to reflect the changes made to the image settings.

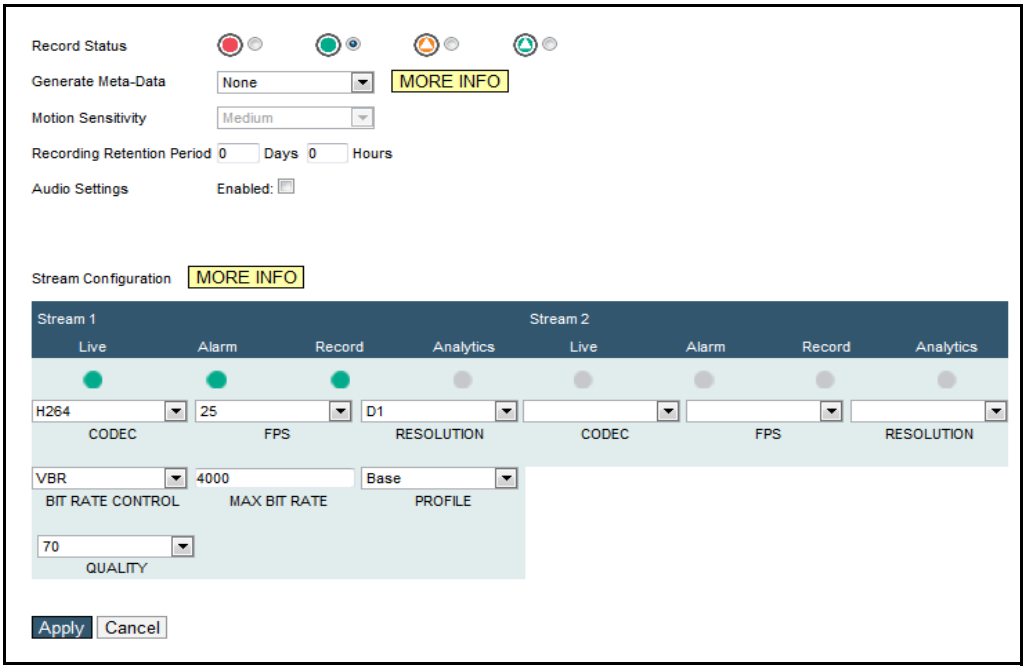
**- End -**

## Configure Camera Function and Stream Settings

The Function and Stream camera settings section is where you configure:

- Camera Recording Status
- Motion Detection
- Motion Sensitivity (Motion Detection only)
- Video Intelligence
- Recording Retention period
- Audio
- Stream Settings

**Figure 8-8 Function and Stream Settings**



## Set the Camera Recording Status

The recording status setting on the camera determines when the camera records. There are 4 recording modes available described in Table 8-1.

### Table 8-1 Recording Statuses

| Mode | Icon | Description |
|---|---|---|
| Recording Off | | Camera is not recording. Live video can still be viewed. |
| Recording Always | | The camera will record continuously. In this mode you will not receive alert notifications from the NVR. |
| Recording Normal Off, Alarm On | | Camera is not recording an alarm is detected recording commences. Using this mode you will receive alert notifications from the NVR. |
| Recording Always with Alarm On | | Camera is recording continuously with alarm detection (bump-on-alarm). Using this mode you will receive alert notifications from the NVR. |

## Procedure 8-7
## Setting the Camera Recording Status

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Click **Setup** in the camera record for which you want to configure camera settings.

The Function & Streams page opens.

4 Select the required **Record Status** option button (Table 8-1 Recording Statuses):

- **Recording Off**
- **Recording Always**
- **Recording Normal Off, Alarms On**
- **Recording Always with Alarm On**

5 Click **Apply**.

**Note**

You can check the recording mode of any camera in the Live Video windows. The recording mode is displayed beside the camera name.

**- End -**

## Set a Camera Recording Retention Period

The recording retention period is the maximum duration over which video recorded for a camera will be saved for, without being deleted. Recorded video older than this will be deleted periodically to free storage space in the storage set the camera is recording to.

### Procedure 8-8
### Setting the Recording Retention Period for a Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Click **Setup** in the camera record for which you want to set the recording retention period.<br>The Function & Streams page opens. |
| 3 | Enter the **Recording Retention Period** in the **Days**, **Hours** and **Minutes** fields. |
| 4 | Click **Apply**. |

**- End -**

## Configuring Camera Audio Settings

You can configure audio settings for cameras that support audio streams. If a camera supports audio streams, an Enabled checkbox is available in the Audio Settings section, in the Function and Stream area of the camera Advanced Edit page. If audio is not supported on a camera, 'Not Supported' displays in the Audio Settings section.

**Note**

Audio playback is not available via the NVR Server Web Interface. The Audio Settings are used to determine how audio streams are made available to victor unified client.

Audio and video are derived from the camera as two separate packet streams. Depending on the camera manufacturer and video/audio codec combination, these data streams may not be exactly in synchronization for live streaming. The NVR's live streaming method is to pull video and audio from the camera and push it to the client straight away. This helps achieve low video latency but sometimes at the expense of live audio/video synchronization. Recorded playback of the same audio and video may give better audio/video synchronization results.

### Procedure 8-9
### Configuring Camera Audio Settings

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click **Setup** in the camera record for which you want to edit audio settings.<br>The Function & Streams page opens. |
| 4 | Select the Audio Settings **Enabled** checkbox. |

CODEC, VOLUME and BIT RATE drop-down lists display.

5 Select the required codec from the **Codec** dropdown list.

**Note**

1 Some camera models do not support all of the audio codecs supported by the NVR.

6 Select the volume from the **Volume** dropdown list.

**Note**

1 The volume is only available on supported camera models.

2 The volume range available is dependant on the camera model.

7 Select the bit rate from the **Bit Rate** dropdown list.

**Note**

The bit rate is only available to select on supported cameras.

8 Click **Apply**.

**- End -**

## Configuring Camera Stream Settings

Use the camera Stream Settings to define which stream is used for live video, alarms and recording. The NVR will automatically determine the best stream to use for Motion Detection or Video Intelligence. You can also adjust the codec, FPS and resolution of each stream. Depending on what is assigned to a stream, you need to have the appropriate codec, FPS and resolution assigned. For example, the stream you are using for Video Intelligence analytics must be MP4V or MPEG, with a recommended resolution of CIF and 7 FPS.

**Note**

If the camera supports only a single stream, the Stream 2 settings for Live Stream, Alarm Stream, Record Stream and Analytics Stream are unavailable.

### Procedure 8-10
### Configuring Stream Settings

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Click **Setup** in the camera record for which you want to edit stream settings.

The Function & Streams page opens.

4 Select the stream you want the camera to use for:

a Live video

b Alarms

c Recording

5 Select the **Codec** for each stream.

6 Select the **FPS** for each stream.

7 Select the **Resolution** for each stream.

8 If you are using a stream for analytics, select the **Quality**.

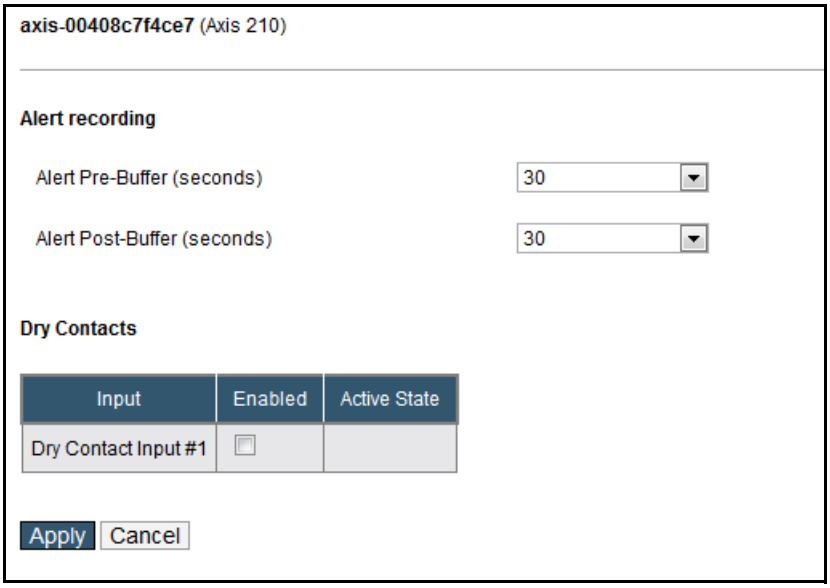
9 Click **Apply.**

**- End -**

# Configuring Alert Buffer Settings

Use the Alerts section to configure pre-alert and post-alert recording buffer times. Buffer times range from 30 seconds to 300 seconds, defined in 10 second intervals.

**Figure 8-9 Alert Tab**




## Procedure 8-11
## Configuring Alert Recording Buffers

**Step Action**

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Click **Setup** in the camera record for which you want to set alert recording buffers.

The Function & Streams page opens.

4 Select **Alerts** tab.

5 Select the **Alert Pre-Buffer** from the dropdown list (range 30 - 300 seconds).

6 Select the **Alert Post-Buffer** from the dropdown list (range 30 - 300 seconds).

7 Click **Apply**.

**- End -**

# Configuring Sensors

## Dry Contact Sensors

You can associate dry contact sensors with a particular camera in the Alerts section. These are sensors typically used in doorways, and are activated, for example, when a door is opened, the NVRs can command cameras to pan-tilt-zoom to predetermined locations and record video for a specified period.

### Procedure 8-12
### Enabling a Dry Contact Sensor

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

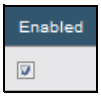
2 Select **List**.

3 Select **Setup** for the camera for which you want to enable dry contact settings.

The Function & Streams page opens.

4 Select **Alerts** tab.

5 Select the Dry Contact Input **Enabled** checkbox(es) in the Dry Contacts section.




6 Click **Apply**.

**Note**

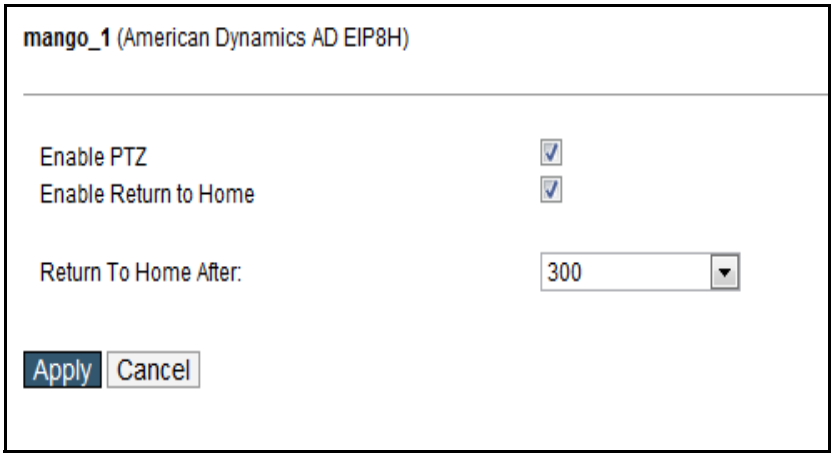
If you are editing the dry contact settings for a camera, forming part of an encoder device, all cameras related to this device will be updated with the changes made to the dry contacts. In this instance, a warning message opens informing you that multiple cameras will be updated.

**- End -**

# Configuring PTZ Settings

If a camera has PTZ capabilities you will be able enable/disable PTZ functionality and configure the Return to Home settings for the camera, otherwise a message stating PTZ is not supported is displayed.

**Figure 8-10 PTZ Settings**




## Enable/Disable PTZ Functionality

You can enable or disable PTZ functionality for a camera provided the camera has PTZ capabilities.

### Procedure 8-13
### Enable or Disable PTZ

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click **Setup** in the PTZ camera record.<br>The Function & Streams page opens. |
| 4 | Select **PTZ** tab. |
| 5 | Select the **Enable PTZ** checkbox to enable PTZ.<br>Or<br>Deselect the **Enable PTZ** checkbox to disable PTZ. |
| 6 | Click **Apply**. |

**- End -**

## Return to Home

When the PTZ Return to Home feature is enabled, this will return the PTZ to its 'home' position after a defined period of inactivity. The first preset in a list of configured presets is considered to be the home position.

When the PTZ is moved the idle timer for the camera is reset. For example, if a camera moves to a preset position, moves using the pan or tilt controls or moves as part of a tour, the idle timer will reset to zero.

**Note**

If the camera is moved using the camera's own web browser controls, the timer will not reset.

The Return to Home period is defined using the dropdown list. The periods available are in seconds between 60 and 600, in 60 second intervals.

### Procedure 8-14
### Enabling PTZ 'Return to Home'

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click **Setup** in the PTZ camera record for which you want to enable the 'Return to Home' feature.<br>The Function & Streams page opens. |
| 4 | Select **PTZ** tab. |
| 5 | Select the Enable PTZ checkbox.<br>**Note**<br>PTZ must be enabled to configure Return to Home settings. |
| 6 | Select the **Enable Return to Home** checkbox.<br>The Return to Home After dropdown displays. |
| 7 | Select the desired period of inactivity before the camera 'returns to home' from the **Return to Home After** dropdown list (range 60 - 600 seconds). |
| 8 | Click **Apply**. |

**- End -**

# Motion Detection

## Overview

The NVR provides server-based motion detection for all cameras. Hardware-based (camera-based) Motion Detection is not supported by the NVR. The NVR supports two motion detection features:

- Motion Search - a victor client can search recorded video for motion.
- Motion Alerts - you can define Motion detection settings that can be used to set up motion detection rules.

The Motion Detection settings allow you to define the parameters which will initiate an alarm. This will reduce the number of unwanted alarm events and is achieved using the following tools:

- Duration settings allowing you to define the time period of activity in the region of interest to activate an alarm.
- Direction settings allowing you to define the direction of motion required to activate an alarm.
- Size expressed as the minimum percentage of the region of interest with activity required before activating an alarm.

Motion Detection provides useful information only if recording is enabled on the camera. Your camera recording status should be set to either Recording Normal Off, Alarm On or Recording Always with Alarm On. For further information on camera recording modes refer to Procedure 8-7 Setting the Camera Recording Status on page 95.

Motion Detection events will create entries in the victor site manager database. If required you can use the Reports feature in victor unified client to retrieve event information.

## Motion Detection Best Practices

To ensure you get the highest quality results when using Motion Detection on the NVR it is recommended that you adhere to the following:

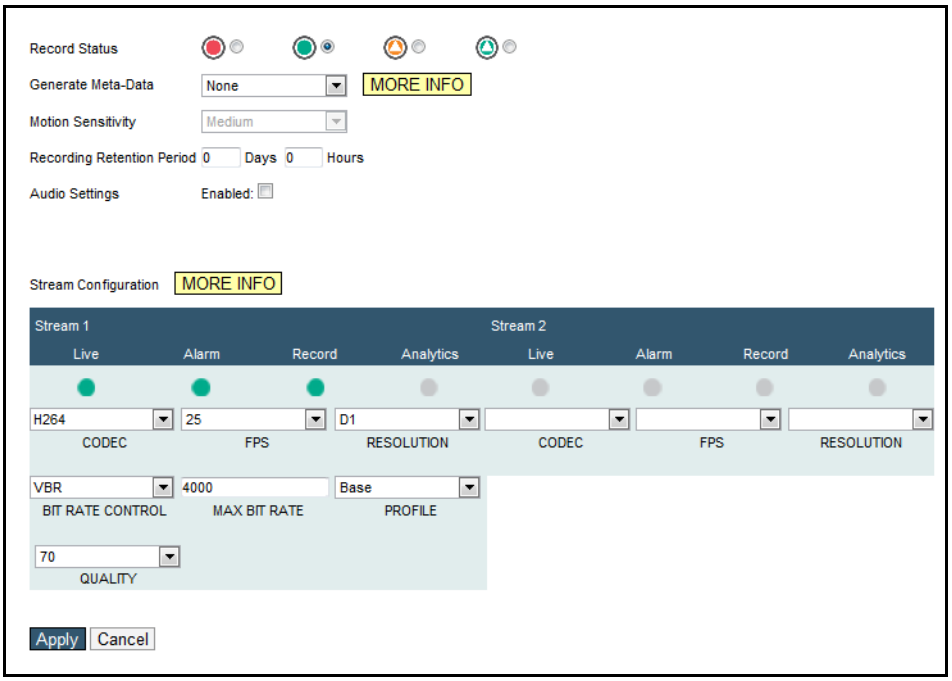
- An object exhibiting motion needs to be at least 8x8 pixels in size to be detected.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.
- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Motion Detection events create entries in the victor site manager database. It is important to ensure that the motion detection parameters are accurate to avoid generating false entries.

- Exclude the Time Stamp region from motion detection, because the time stamp changes constantly and could register as motion.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Do not use motion detection on moving cameras, such as PTZ cameras, cameras that vibrate due to wind or other effects, or cameras mounted on moveable fixtures.

# Enabling Motion Detection

To enable a camera to use Motion Detection features, you can use the Camera List page. Refer to Procedure 8-1 Editing Basic Camera Settings via the Camera List on page 85 or the Function and Stream settings section of the camera Advanced Edit page.

**Figure 9-1 Function and Stream Settings**




A Stream Configuration is required that allows the NVR to generate meta-data for motion detection. You also need to select **Motion Detection** in the **Generate Meta-Data** field. The NVR will automatically determine the required stream settings (Table 9-1) and check if the currently configured streams satisfy those requirements. If only one stream is configured and it does not satisfy the requirements for Motion Detection, the NVR will attempt to automatically open the second stream with settings best suited for Motion Detection. If the camera does not support dual streaming you will manually need to adjust the configuration of the configured stream.

Motion Detection may not be available on a camera if it's minimum video resolution setting is higher than the maximum acceptable resolution for Motion Detection. The NVR will not allow you to configure a camera for Motion Detection if the resolution setting of the camera is higher than the settings in Table 9-1.

### Table 9-1 Camera Resolutions for Motion Detection

| Camera Type | Minimum Resolution | Maximum Resolution |
|---|---|---|
| MJPEG | QCIF | 1280 x 960 |
| MP4V | QCIF | CIF |

The optimal stream to perform Motion Detection is 320 x 240 resolution (or the closest resolution supported by the camera), MJPEG at 7 frames per second. Lower resolution or framerates might degrade the quality of Motion Detection. The NVR requires at least QCIF and more than 4 frames per second to perform motion detection.

## Procedure 9-1
## Enabling Motion Detection for a Camera

**Step** **Action**

**1** Select **Cameras** from the main menu.

**2** Select **List**.

**3** Click **Setup** in the camera record for which you want to configure camera settings.

The Function & Streams page opens.

**Note**

You can also enable Motion Detection from the Camera List, refer to Procedure 8-1 Editing Basic Camera Settings via the Camera List on page 85.

**4** Set the camera **Record Status** to a setting that supports Motion Detection ( Recording Normal Off, Alarm On or Recording Always with Alarm On).

**5** Select **Motion Detection** from the **Generate Meta-Data** dropdown list.

**Note**

If an error message opens, the NVR cannot detect a suitable stream from the camera to support Motion Detection. You will need to change the Codec Image Resolution, or FPS of one of your camera's streams to settings that are compatible with Motion Detection, see Table 9-1.

**6** Select the required level of **Motion Sensitivity**. Values range from High (most results) to Low (least results).

**7** Click **Apply**.

**8** To create a Motion Detection alarm, refer to Procedure 9-3 Creating a Motion Detection Camera Alarm on page 108.

**- End -**

# Disabling Motion Detection

When required, you can disable Motion Detection in the Camera List or using the camera's Advanced Edit page. When Motion Detection is disabled you will not be able to perform some of the Motion Detection based activities, such as setting NVR Motion Detection alarms.

### Procedure 9-2
### Disabling Motion Detection for a Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **List**. |
| 3 | Click **Setup** in the camera record where you want to disable camera Video Intelligence.<br>The Function & Streams page opens. |
| 4 | Select **None** from the **Generate Meta-Data** dropdown list. |
| 5 | Click **Apply**. |

**- End -**

# Motion Detection Alarms

After enabling Motion Detection on a camera, you can set alarm rules that trigger an event.

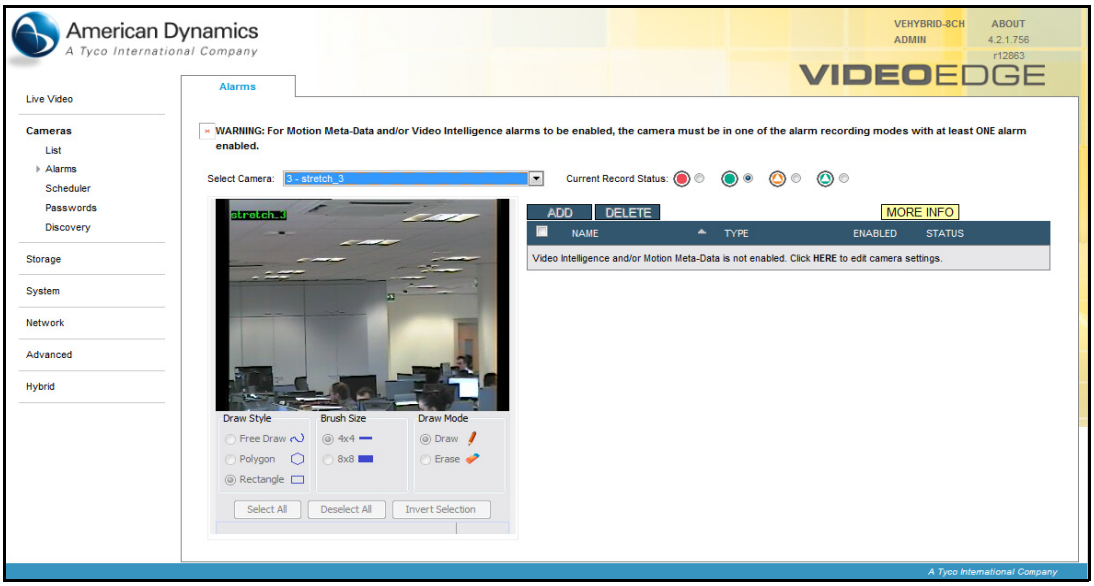
Each camera can have up to 10 independent motion alarm rules defined. Each rule has an associated region of interest. In each region of interest you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like 'Back Door' or 'Conference Room', as these names make it easier to identify the alarm in victor reports better than an abstract name.

The areas that you want to monitor in a cameras view are configured in the Camera Alarm Configuration drawing window, a live display of the camera view. To determine the areas of the camera view that you want monitored you need to draw on the window. Use the drawing tools to draw on the Camera Alarm Configuration window.

The status of each Video Intelligence alarm highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Recording Normal Off, Alarm On** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

## Figure 9-2 Camera Alarm Configuration




## Table 9-2 Drawing Tools

| Tool Type | Options | Description |
|---|---|---|
| Draw Style | Free Draw | Draw using free draw by clicking on the window and dragging to draw the shape. The detection area is highlighted in yellow. |
| | Polygon | Draw a polygon by clicking once in the window, and use the lines to form the region of interest. Click again to confirm the line. Double click when the shape is complete to finalise the detection area. The detection area is highlighted in yellow. |
| | Rectangle | Draw a rectangle by clicking once in the window and dragging the cursor over the camera view to highlight the area of interest. The detection area is highlighted in yellow when the mouse button is released. |

| Tool Type | Options | Description |
|---|---|---|
| Brush Size | 4 x 4 | You can choose the brush size when using free draw to draw a region of interest for Video Intelligence alarms. Select 4 x4 to draw using a thin line.<br><br>**Note**<br>This option is not available when configuring Motion Detection alarms. |
| | 8 x 8 | You can choose the brush size when using free draw to draw a region of interest for Video Intelligence alarms. Select 8 x 8 to draw using a thick line.<br><br>**Note**<br>This option is not available when configuring Motion Detection alarms. |
| Draw Mode | Draw | Select Draw when you want the draw style to draw a detection area. |
| | Erase | Select Erase when you want the draw style to erase sections of a detection area. |

## Creating a Motion Detection Camera Alarm

When creating Motion Detection camera alarm you must define an alarm rule. When activity in a camera's view or region of interest satisfies the criteria defined in the rule, an alarm is triggered.

To create a Motion Detection camera alarm you must have Motion Detection enabled on the camera (Procedure 9-1 Enabling Motion Detection for a Camera). If you try to add a camera alarm without Motion Detection enabled you will be prompted to edit the camera settings.

### Procedure 9-3
### Creating a Motion Detection Camera Alarm

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Alarms**.<br><br>The Camera Alarm Configuration page opens (Figure 9-2). |
| 3 | Select the camera for which you want to create an alarm, from the **Select Camera** dropdown list. |
| 4 | Click **Add**.<br><br>**Note**<br>If the **Add** button is not available, you do not have Motion Detection or Video Intelligence enabled on the camera. Enable Motion Detection to continue, refer to Procedure 9-1 Enabling Motion Detection for a Camera. |

5 If required you can update the **Current Record Status**. For Motion Detection to be enabled you must select either **Recording Normal Off, Alarm On** or **Recording Always with Alarm On**, refer to Table 8-1 Recording Statuses on page 95 for further information.

6 Enter an alarm **Name** (max 50 characters).

**Note**

Use a descriptive name that will make the alarm easy to identify.

7 Ensure **Motion** is the selected **Type**.

**Note**

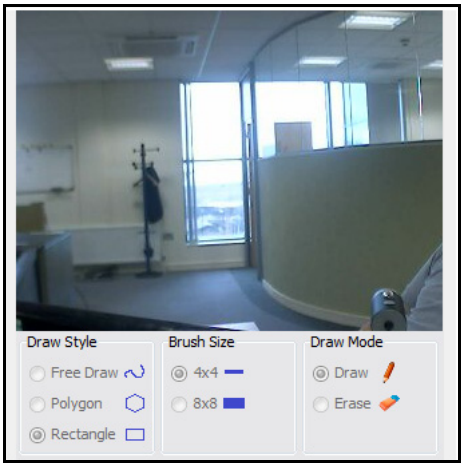
If the **Motion** is not available in the dropdown list, you do not have Motion Detection enabled on the camera, instead Video Intelligence is enabled. Enable Motion Detection to continue, refer to Procedure 9-1 Enabling Motion Detection for a Camera.

8 (Optional) Use the drawing tools to draw the Motion Detection region of interest in the Camera Alarm Configuration drawing window. Refer to Table 9-2 for information on how to use the drawing tools.

**Note**

If you do not draw a region of interest, the entire camera view will be used as the region of interest.

**Figure 9-3 Camera Alarm Configuration Drawing Window**




9 Select the **Yes** option button for the **Enabled** field, to enable the alarm.

10 Use the **Size (%)** slider to determine the percentage of the region of interest with activity present for the alarm to be triggered. The higher the percentage of the region of interest selected, the lower the number of motion detection results triggered for the alarm. A setting of 0% will trigger an alarm for any size motion.

11 Enter the **Duration (secs)** that there is sustained activity in the region of interest before the alarm is triggered. You can enter values between 0 (default) and 600. A value of 0 seconds will trigger an alarm for motion of any duration.

12 Select the **Direction** from the dropdown list that the center of the activity area of motion must move, in order to trigger the alarm. If you select **ANY** it will trigger an alarm for movement in any direction.

13 Select **Save**.

**- End -**

## Editing a Motion Detection Camera Alarm

You can make changes to camera alarm settings if required, for example, you can change the region of interest, the percentage of the region of interest that requires activity present, the duration of activity or the direction of movement.

### Procedure 9-4
### Editing a Motion Detection Camera Alarm

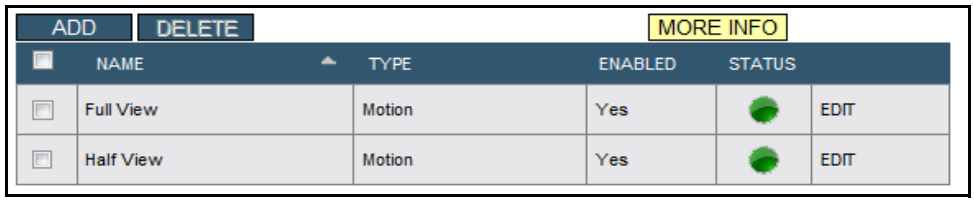
| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **Alarms**.

The Camera Alarm Configuration page opens (Figure 9-2).

3 Select **Edit** for the camera alarm you want to edit.




4 Use the drawing tools to edit the Motion Detection region of interest in the Camera Alarm Configuration drawing window. Refer to Table 9-2 for information on how to use the drawing tools.

5 Use the **Size (%)** slider to edit he percentage of the region of interest with activity present for the alarm to be triggered. The higher the percentage of the region of interest selected, the lower the number of motion detection results triggered for the alarm. A setting of 0% will trigger an alarm for any size motion.

6 Edit the **Duration (secs)** that there is sustained activity in the region of interest before the alarm is triggered. You can enter values between 0 (default) and 600. A value of 0 seconds will trigger an alarm for motion of any duration.

7 Edit the **Direction** by selecting a different direction from the dropdown list. The direction is the center of the activity area of motion must move, in order to trigger the alarm. If you select **ANY** it will trigger an alarm for movement in any direction.

8 Select **Save**.

**- End -**

## Disabling a Motion Detection Camera Alarm

When a Motion Detection camera alarm is not needed at present, but will be needed in the future, the alarm can be disabled. The alarm configuration remains the same on the camera for when it is enabled again.

### Procedure 9-5
### Disabling a Camera Alarm

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Alarms**.<br>The Camera Alarm Configuration page opens (Figure 9-2). |
| 3 | Select the alarm record you want to disable. |
| 4 | Click **Edit**. |
| 5 | Select the **No** option button in the **Enabled** field. |
| 6 | Click **Save**. |

**- End -**

## Deleting a Motion Detection Camera Alarm

When a Motion Detection camera alarm is no longer required, it can be deleted.

### Procedure 9-6
### Deleting a Camera Alarm

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Alarms**.<br>The Camera Alarm Configuration page opens (Figure 9-2). |
| 3 | Select the alarm record you want to delete. |
| 4 | Click **Delete**.<br>The alarm record is removed from the alarm table. |

**- End -**

# Video Intelligence

## Overview

The NVR provides server based Video Intelligence for all cameras. Video Intelligence is a licenced add-on for the NVR. Hardware-based (camera-based) Video Intelligence is not supported by the NVR. The NVR supports two Video Intelligence features:

- Video Intelligence Search - a victor client can search recorded video for a specific type of event. Refer to the victor Configuration and User Guide for further information on Video Intelligence searches.
- Video Intelligence Alerts - you can define Video Intelligence settings that can be used to set up Video Intelligence rules.

There are several types of Video Intelligence rules available. These include:

- **Object Detection** - Used to detect people or objects moving into a region of interest. This search is similar to a motion search, but only detects people or objects on entry of the region of interest i.e. they will not be continuously detected if they remain within the region of interest. If the object leaves the camera view and returns, the search will detect them again. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.
- **Object Direction** - Used to detect objects moving in a certain direction through a region of interest, for example, a car travelling the wrong way on a road.
- **Object Linger** - Used to detect objects lingering in an area of interest. An object is lingering if it is mostly stationary.
- **Object Enter** - Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold.
- **Object Exit** - Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold.
- **Object Abandoned/Removed** - Used to find changes to the background of a scene in a region of interest, for example, use it to detect when a stationary object was placed, moved or removed.

The Video Intelligence settings allow you to define the parameters which will initiate an alarm (an alarm rule). This will reduce the number of unwanted alarm events. The parameters available are dependent on the type of Video Intelligence rules which are defined.

Video Intelligence provides useful information only if recording is enabled on the camera. Your camera should be configured with **Recording Normal Off, Alarm On** or **Recording Always with Alarm On** recording modes. For further information on camera recording modes refer to Table 7-1 Camera List Summary on page 77.

Video Intelligence events will create entries in the victor site manager database. If required you can use the Reports feature in victor unified client to retrieve event information.

To carry out Video Intelligence based activities you need to enable Video Intelligence on the NVR.

## Video Intelligence Best Practices

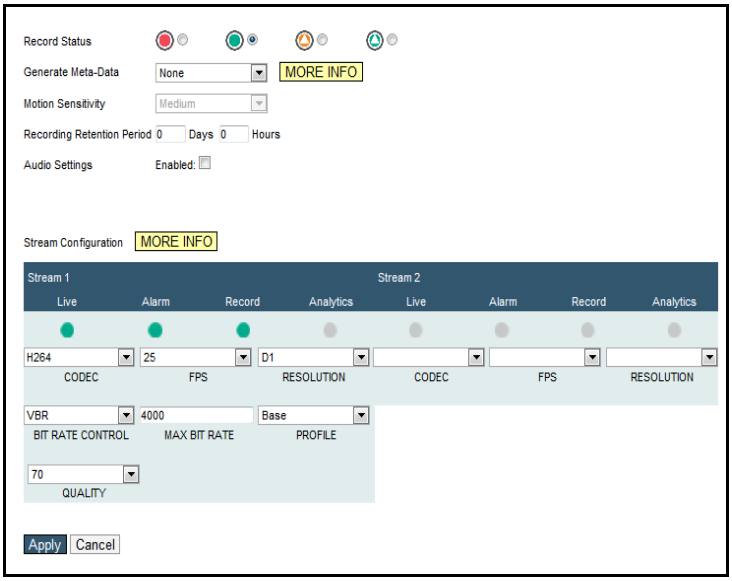
To ensure you get the highest quality results when using Video Intelligence on the NVR it is recommended that you adhere to the following:

- An object exhibiting movement or a change in the scene background must be large enough to be detected, i.e. it must be around 1/25 of the image size.
- The color of the object (in grayscale) should be approximately 10-15% different than the background.
- The frame rate of the video should be high enough to capture the object in one or more captured frames.
- Video Intelligence events create entries in the victor site manager database. It is important to ensure that the Video Intelligence parameters are accurate to avoid generating false log entries.
- Exclude the Time Stamp region from the region of interest, because the time stamp changes constantly and could register as movement.
- Try not to point cameras into sunlight, because high brightness will prevent detection of movement of bright objects such as a person with a white shirt.
- Avoid areas with persistent motion, such as trees, blinking lights, or spinning signs, by using an appropriate region of interest.
- Do not use Video Intelligence on moving cameras, such as PTZ cameras, cameras that vibrate due to wind or other effects, or cameras mounted on moveable fixtures.
- Choose your Video Intelligence alarms selectively. You do not want to create alarms that will trigger a high number of alerts, making the important alerts more difficult to identify.
- Situate cameras to provide the best possible views of the areas of interest, objects and people. It is best to ensure camera views separate objects from people, ensure objects and people take up a larger portion of the camera view, and keep the entire region of interest within the camera's view.
- Use the scheduler to ensure alarm recording statuses are activated at night or during non working hours. This provides additional coverage during times when staff are not normally available. For further information on the scheduler and recording modes, refer to Camera Scheduler on page 123.
- Use staff to help identify regions of interest to monitor based on their observations, for example, of missing merchandise or missing fixtures. Video Intelligence alarms can therefore be configured to monitor areas of potential activity.
- Use searches frequently and watch activity leading up to an alarm being triggered. This may give an indication of suspicious activity and other areas to monitor.
- Tune your alarms regularly to ensure the alarms reflect changes to the environment, for example, objects being rearranged or replaced. Monitoring these changes and re-tuning your alarms will ensure maximum effectiveness of the Video Intelligence alarms and searches.
- Use the new information that Video Intelligence provides to learn and adapt. Use it to implement changes that will improve surveillance and reduce losses, for example, eliminate blind spots, make staff aware of suspicious behavior, or re-design the environment and alarms.

# Enable Video Intelligence for a Camera

To enable a camera to use Video Intelligence features, you can use the Camera List Page or the Function and Stream settings section of the camera Advanced Edit page.

**Figure 10-1 Function and Stream Settings**




You must ensure you have a Stream Specification that allows the NVR to generate meta-data for Video Intelligence. You also need to select **Video Intelligence** in the **Generate Meta-Data** field.

The NVR will automatically determine the required settings and apply them to a stream. If the camera is configured for dual-stream, then the NVR chooses the best stream. If the NVR is unable to find a suitable video stream for Video Intelligence an error message opens.

Video intelligence may not be available for a particular camera if the camera's video resolution setting is lower than the minimum or higher than the maximum acceptable resolution for Video Intelligence. The NVR will not allow you to configure a camera for Video Intelligence if the resolution setting of the camera is outside of the settings in Table 10-1.

**Table 10-1 Camera Resolutions for Video Intelligence**

| Camera Type | Minimum Resolution | Maximum Resolution |
|---|---|---|
| MJPEG | 320 x 180 | 1280 x 960 |
| MP4V | 320 x 180 | CIF |

The optimal stream to perform Video Intelligence is CIF (320 x 240 resolution) MJPEG at 7 frames per second. The NVR requires at least 320 x 180 resolution and more than 4 frames per second to perform Video Intelligence activities.

## Procedure 10-1
## Enabling Video Intelligence for a Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |

2 Select **List.**

3 Click **Setup** in the camera record for which you want to enable Video Intelligence.

The Function & Streams page opens.

**Note**

You can also enable Video Intelligence from the Camera List, refer to Procedure 8-1 Editing Basic Camera Settings via the Camera List on page 85.

4 Set the camera **Record Status** to a setting that supports Video Intelligence ( Recording Normal Off, Alarm On or Recording Always with Alarm On).

5 Select **Video Intelligence** from the **Generate Meta-Data** dropdown list.

**Note**

If an error message opens, the NVR cannot detect a suitable stream from the camera to support Video Intelligence. You will need to change the Codec, Image Resolution, or FPS of one of your camera's streams to settings that are compatible with Video Intelligence, refer to Table 10-1.

6 Click **Apply**.

7 To create a Video Intelligence alarm, refer to Procedure 10-3 Creating a Video Intelligence Camera Alarm on page 118.

**- End -**

# Disable Video Intelligence for a Camera

If you do not want Video Intelligence activities carried out on a camera, you can disable Video Intelligence in the NVR camera settings. When Video Intelligence is disabled you will not be able to perform any Video Intelligence searches or set Video Intelligence alarms on the camera. However, the Video Intelligence alarms defined on a camera are remembered and will become active if Video Intelligence is enabled again for that camera.

## Procedure 10-2
## Disabling Video Intelligence for a Camera

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **List**.

3 Click **Setup** in the camera record where you want to disable camera Video Intelligence.

The Function & Streams page opens.

4 Select **None** from the **Generate Meta-Data** dropdown list.

5 Click **Apply**.

**- End -**

# Video Intelligence Camera Alarms

After enabling Video Intelligence on a camera, you can define alarm rules that trigger an event.

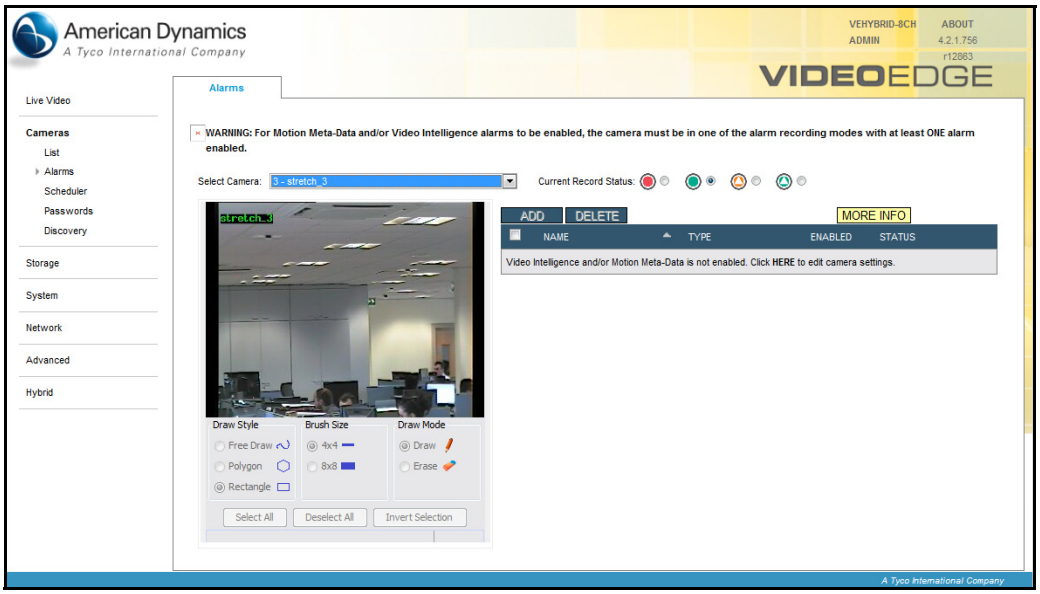
Each camera can have any number of independent Video Intelligence rules. In each rule you can define the areas in the cameras view that you want to monitor. You can name each alarm rule. It is best to use descriptive names like ‘Back Door’ or ‘Conference Room’, as these names make it easier to identify the alarm rule in the alerts log better than an abstract name. You can choose the Video Intelligence type for the rule.

The areas that you want to monitor in a cameras view are configured in the Camera Alarm Configuration drawing window, a live display of the camera view. To determine the areas of the camera view that you want monitored you need to draw on the window. Use the drawing tools to draw on the Camera Alarm Configuration window.

The status of each Video Intelligence alarm highlighted in the **Status** field. There are three alarm states:

- **Red** - Alarm is disabled. The alarm can be disabled via the **Enabled** option button.
- **Yellow** - Alarm is enabled, however, the recording mode set for the camera does NOT support alarms so the alarms will not be generated. Supported modes are **Recording Normal Off, Alarm On** or **Recording Always with Alarm On**.
- **Green** - Alarm is enabled and a supported recording mode is selected. Alarms will be generated.

Figure 10-2 Camera Alarm Configuration




## Creating a Video Intelligence Camera Alarm

To create a Video Intelligence camera alarm you must have Video Intelligence enabled on the camera, refer to Procedure 10-1 Enabling Video Intelligence for a Camera on page 115.

**Note**

If you try to create a Video Intelligence alarm for a camera without Motion Detection or Video Intelligence enabled you will be prompted to edit the camera settings.

### Procedure 10-3
### Creating a Video Intelligence Camera Alarm

| Step | Action |
|---|---|
| 1 | Select **Cameras** in the main menu. |
| 2 | Select **Alarms**.<br>The Camera Alarm Configuration page opens (Figure 10-2). |
| 3 | Select the camera for which you want to create a Video Intelligence alarm from the **Select Camera** dropdown list. |
| 4 | Click **Add**.<br>**Note**<br>If the **Add** button is not available, you do not have Motion Detection or Video Intelligence enabled on the camera. Enable Video Intelligence to continue, refer to Procedure 10-1 Enabling Video Intelligence for a Camera. |
| 5 | If required you can update the **Current Record Status**. For Video Intelligence alarms to be enabled you must select either **Recording Normal Off, Alarm On** or **Recording Always with Alarm On**, refer to Table 8-1 Recording Statuses on page 95 for further |

information.

6 Enter an alarm **Name** (max 50 characters).

**Note**

Use a descriptive name that will make the alarm easy to identify.

7 Select the Video Intelligence **Type** from the dropdown list:

- **a** **Object Detection** - Used to detect people or objects moving into a region of interest. This alarm is similar to a motion alarm, but only detects people or objects the first time they enter the region of interest. A separate event is generated for each object that enters the region, even if the objects move into the region at the same time, unlike motion detection that generates one event.
- **b** **Abandoned / Removed** - Used to find changes to the background of a scene in a region of interest, for example, use it to detect when a stationary object was placed, moved or removed. Draw the region of interest that contains all of the area you want to search for changes.
- **c** **Direction** - Used to detect objects moving in a certain direction through a region of interest, for example, a car travelling the wrong way on a road. It is best to use a thin region of interest to detect the direction of an object.
- **d** **Linger** - Used to detect objects lingering in an area of interest. An object is lingering if it is mostly stationary.
- **e** **Exit** - Used to detect objects exiting a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.
- **f** **Enter** - Used to detect objects entering a camera view through a region of interest, for example, a doorway or threshold. It is best to draw the region of interest around the doorway or threshold to include areas in which the door can move or objects can be seen, for example, glass. This will exclude objects that can be seen in the region of interest but does not pass through it.

**Note**

If these types are not available in the dropdown list, you do not have Video Intelligence enabled on the camera, instead Motion Detection is enabled. Enable Video Intelligence to continue (Procedure 10-1 Enabling Video Intelligence for a Camera on page 115).

8 (Optional) Use the drawing tools to draw the Video Intelligence region of interest in the Camera Alarm Configuration drawing window, refer to Table 9-2 Drawing Tools on page 107 for information.

**Note**

If you do not draw a region of interest, the entire camera view will be used as the region of interest.

9 Enable the alarm by selecting the **Yes** option button for the **Enabled** field.

10 Complete the alarm configuration fields. Depending on the Video Intelligence type selected there will be different alarm parameters to configure:

**Object Detection**

**a** Overlap (%) - The amount of a detected object that must be in the region of interest before an alarm is triggered. Use a higher setting to detect objects that are mostly inside the region, and use a lower value to find objects that just brush the edge of the region.

**Abandoned / Removed**

**a** Overlap (%) - The amount of background change that must be in the region of interest before an alarm is triggered. Use a higher setting to avoid finding nearby changes or changes that are not completely in the region of interest.

**b** Wipeout Amount Changed (%) - The percentage of the region of interest that must change before an alarm is triggered. Adjust to look for either a larger or smaller change in the region.

**c** Wipeout Within (secs) - Time frame within which the change must occur in order to trigger the alarm. A setting of 0 seconds represents instantaneous change.

**Direction**

**a** Overlap (%) - The amount of a detected object that must be in the region of interest while moving in the specified direction for an alarm to be triggered.

**b** Direction - This is the general direction the object must move in to trigger an alarm. You can choose North, South, East or West.

**c** Traversal Time- This is the maximum amount of time which an object can take to traverse most of the region before the alarm is triggered. This is to exclude objects that move too slow.

**Linger**

**a** Overlap (%) - The amount of detected object that must be in the region of interest while lingering for an alarm to be triggered. Use a higher setting to avoid detecting objects lingering nearby.

**b** Linger Time- The minimum amount of time an object lingers before the alarm is triggered.

**Exit**

**a** Overlap (%) - The amount of detected object that must be in the region of interest when the object leaves the scene for an alarm to be triggered. The object must appear in the scene while being outside the region of interest by the same amount. For best results select a higher overlap setting.

**Enter**

**a** Overlap (%) - The amount of detected object that must be in the region of interest when it first appears in the camera view. The object must leave the region of interest by the same amount before an alarm is triggered. For best results select a higher overlap setting.

**11** Click **Save**.

**- End -**

## Editing a Video Intelligence Camera Alarm

You can make changes to Video Intelligence camera alarm rules if required, for example, you can change the region of interest and update the parameters associated with that rule's Video Intelligence alarm type.

### Procedure 10-4
### Editing a Motion Detection Camera Alarm

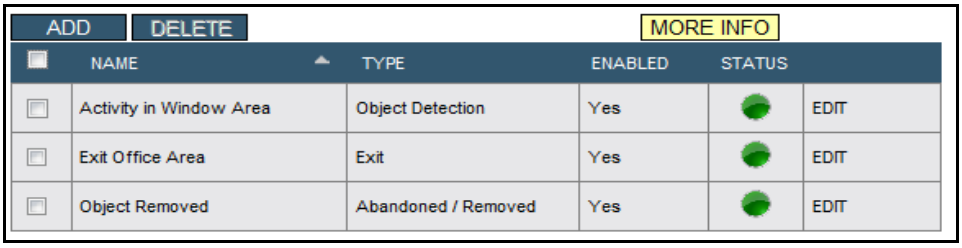
| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **Alarms**.

The Camera Alarm Configuration page opens (Figure 10-2).

3 Select **Edit** for the camera alarm you want to edit.




4 Use the drawing tools to edit the selected alarm's region of interest in the Camera Alarm Configuration drawing window, refer to Table 9-2 Drawing Tools on page 107 for information on how to use the drawing tools.

5 Edit the alarm's parameters. These will be different for each type of Video Intelligence alarm.

**Note**

You cannot update the Name of the alarm. If you must change the alarm name, you must create a new alarm with the new name, assign it the same parameters and delete the old alarm.

6 Select **Save**.

**- End -**

## Disabling Video Intelligence Camera Alarm

When a Video Intelligence camera alarm is not needed at present, but will be needed in the future, the alarm can be disabled. The alarm configuration remains the same for when it is enabled again. You can also edit the alarm configuration parameters while the alarm is disabled, once enabled the changes will take effect.

### Procedure 10-5
### Disabling a Camera Alarm

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **Alarms**.

The Camera Alarm Configuration page opens (Figure 10-2).

3 Select the alarm record you want to disable.

4 Click **Edit**.

5 Select the **No** option button in the **Enabled** field.

6 Click **Save**.

**- End -**

## Deleting a Video Intelligence Camera Alarm

When a camera alarm is no longer required, it can be deleted.

### Procedure 10-6
### Deleting a Video Intelligence Camera Alarm

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **Alarms**.

The Camera Alarm Configuration page opens (Figure 10-2).

3 Select the alarm record you want to delete.

4 Click **Delete**.

The alarm record is removed from the alarm table.

**- End -**

# Camera Scheduler

## Overview

This chapter describes how to set up and enable the camera scheduler. By using a camera schedule you can set the NVR to automatically change recording modes hourly. You can define camera recording modes and set camera recording times per scheduler group. You can enable or disable the camera scheduler when necessary.

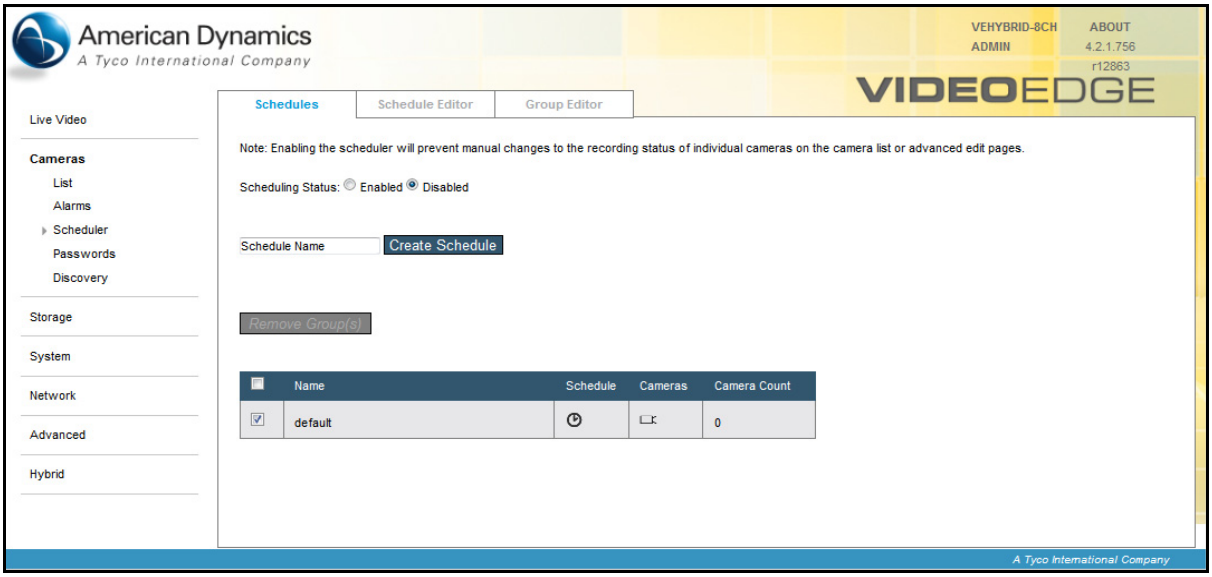
There are three pages within the Scheduler menu; the Schedules page, the Scheduler Editor page and the Group Editor page. A schedule is a collection of cameras with the same recording times. The Schedules page is where you can enable the scheduler and create or remove schedules. The Schedule Editor page is where you set the schedule times and recording modes for each period. The Group Editor page is where you select which cameras belong to a schedule. You can create multiple schedule groups where you can assign different cameras with different schedule times and record modes.

## Create a Recording Schedule

To create a recording schedule you need to:

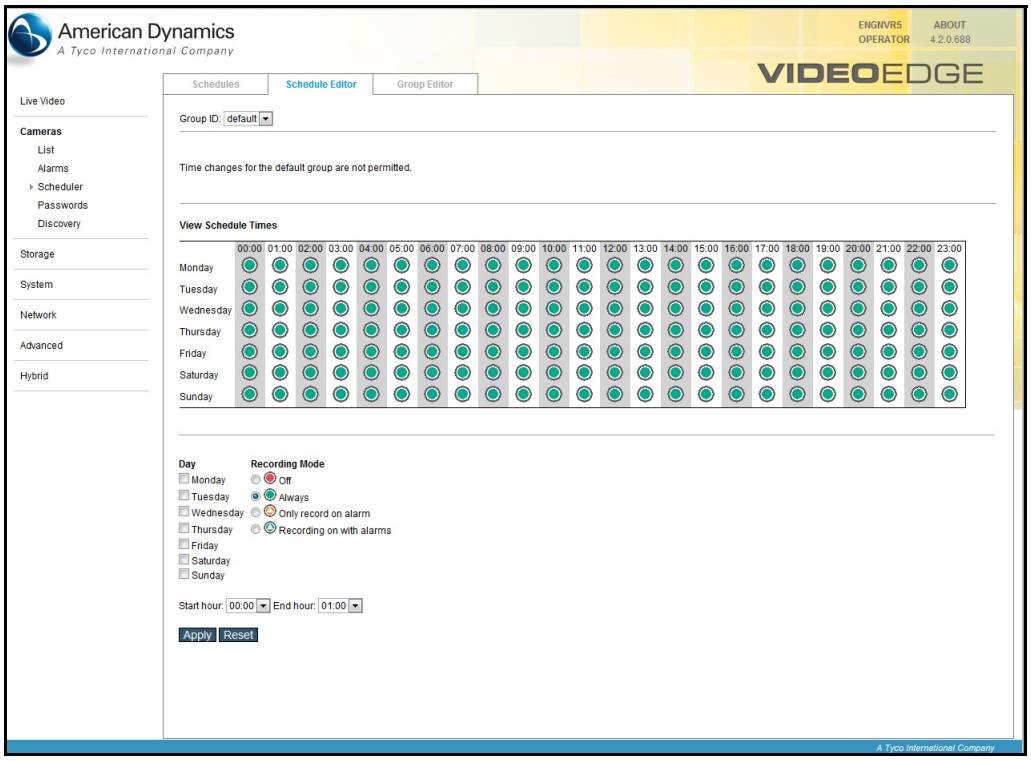
**1** Set up your scheduler group(s).

**Figure 11-1 Schedules Page**



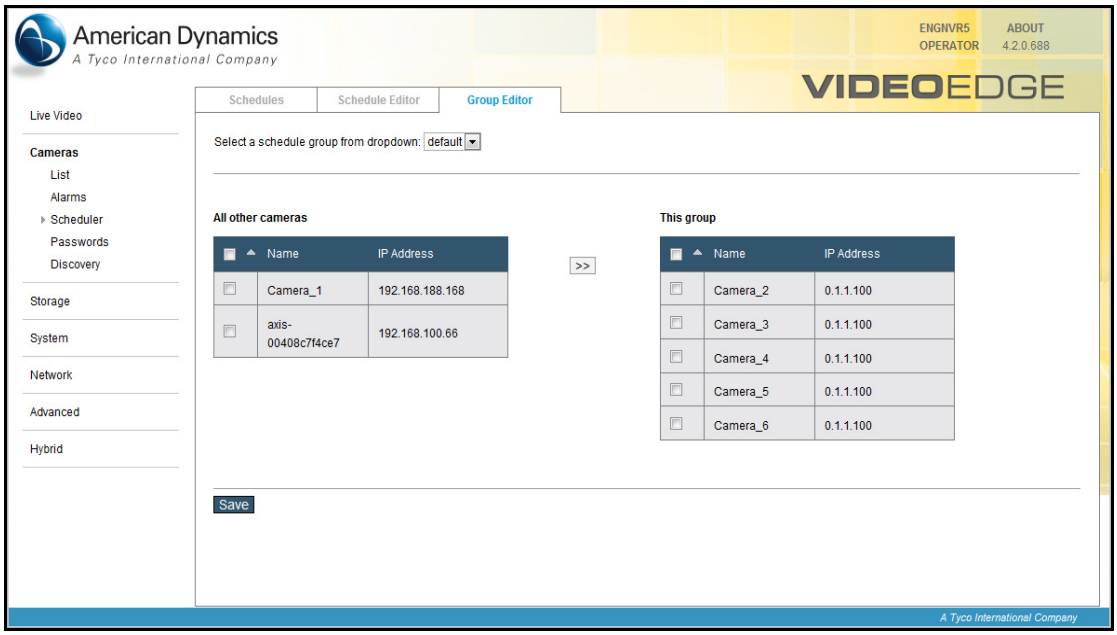

**2** Set the schedule times and recording modes for the schedule group(s).

**Figure 11-2 Schedule Editor Page**




**3** Assign camera(s) to the schedule group(s).

**Figure 11-3 Group Editor Page**




## Procedure 11-1
## Creating a Recording Schedule

| Step | Action |
|---|---|

**1** Select **Cameras** from the main menu.

**2** Select **Scheduler.**

The Schedules page opens.

**3** Create a new schedule group.

**a** Enter a schedule name into the **Schedule Name** field.

**b** Click **Create Schedule**.
The new group is added to the schedule groups table.

**4** Select **Edit Group Times** , in the schedule group record you want to configure.

The Schedule Editor page opens (Figure 11-2).

**5** Select the checkbox(es) representing the day(s) for which you want to set the recording times and the recording mode.

**6** Select the **Recording Mode** option button, you can select;

- **Off**
- **Always**
- **Only record on alarm**
- **Recording on with alarms**

For further information on recording modes refer to Recording Statuses on page 95.

**7** Select the times between which you want the selected recording mode to be active:

**a** Select the **Start hour** from the dropdown.

**b** Select the **End hour** from the dropdown.

8 Click **Apply**.

The Schedule Times chart updates with the selected day(s), recording mode and times.

**Note**

If you click **Apply All Week**, the selected recording mode will be applied to every hour of every day of the week. It will not apply the recording mode and selected start and end times to every day of the week.

9 To set other recording modes for different days and times, repeat steps 5 to 8 until the Schedule Times chart is set as required for the recording schedule group.

10 Select the **Group Editor** tab.

11 Select the cameras you want to be in this schedule group by selecting the checkbox(es) for the cameras from the **All other cameras** list and use the >> arrow to move them to the **This group** list.

**Note**

Each camera can only be assigned to one schedule.

12 Click **Save**.

13 Repeat steps 3 to 12 to configure additional schedule groups for the camera schedule.

**- End -**

# Enabling/Disabling the Recording Schedule

## Procedure 11-2
## Enabling/Disabling a Camera Schedule

| Step | Action |
|---|---|

1 Select **Cameras** from the main menu.

2 Select **Scheduler**.

The Schedules page opens.

3 To enable the camera schedule, select the **Scheduling Status: Enabled** option button.

Or

To disable the camera schedule, select the **Scheduling Status: Disabled** option button.

**- End -**

# Editing the Recording Schedule

If changes need to be made to the recording schedule that has been set up, you can edit all aspects of the recording schedule as required. The following sections describe how to make changes to the recording schedule.

## Edit the Group Name

You may want to update the schedule group name to reflect changes made within the schedule group.

### Procedure 11-3
### Editing the Schedule Group Name

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Scheduler.**<br>The Schedules page opens. |
| 3 | Click **Rename** in the group record that you want to rename.<br>The group name field becomes editable. |
| 4 | Enter the new group name. |
| 5 | Click **Save**. |

**- End -**

## Edit the Recording Scheduler for a Group

Within the recording schedule associated to a group you can update the recording days and times as your needs change. The following procedure describes how to edit the recording schedule.

### Procedure 11-4
### Editing the Recording Schedule for a Group

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu |
| 2 | Select **Scheduler**.<br>The Schedules page opens |
| 3 | Select the **Schedule Editor** tab. |
| 4 | Select the group you want to edit from the **Group ID** drop down. |
| 5 | Edit the recording schedule as required by selecting the day(s), the recording mode and start and end hours. |
| 6 | Click **Apply.** |

7 If further changes are required repeat Steps 5 and 6.

**- End -**

## Edit the Cameras Assigned to a Schedule Group

You can add or remove cameras to/from a schedule group when needed. This procedure describes how to edit cameras assigned to a specific schedule group.

### Procedure 11-5
### Editing the Cameras Assigned to a Schedule Group

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Scheduler.**<br>The Schedules page opens. |
| 3 | Select the **Group Editor** tab. |
| 4 | Select the group you want to edit from the dropdown. |
| 5 | Select the required camera(s) checkbox(es) and use the << and >> arrows to move cameras between the **All other Cameras** list and the **This group** list, until the cameras you want to be assigned to the selected recording group are in the **This group** list. |
| 6 | Click **Save**. |

**- End -**

# Remove a Schedule Group

You can remove unwanted schedule groups when they are no longer needed.

**Note**

If you remove a schedule, the cameras in this schedule will be assigned back to the default scheduler group.

### Procedure 11-6
### Removing a Schedule Group

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Scheduler**.<br>The Schedules page opens. |

3 Select the checkbox in the group record(s) that you want to delete.

4 Select **Remove Group(s)**.

The group is removed from the Schedule groups table.

**- End -**

# Camera Password Groups

## Overview

When an IP camera is added to a NVR, the server uses the manufacturer's default username and password to communicate with the camera. Administrators can change the default security information, however, when this is changed the NVR can no longer communicate with the camera using the default settings.

If you change the password for a camera or a number of cameras, usually through direct web interfaces, you need to create a Password Group for those cameras and assign it the same password. Use the Passwords feature to define the password group that is to be used by the NVR to communicate with a group of cameras.

**Note**

1 The Password feature does not change the password on the camera. It determines what password is used by the NVR to communicate with cameras.

2 You must change the password on the camera before you change the password for the password group using the Passwords feature, otherwise those cameras will not be able to connect to the NVR.

## Create a Password Group

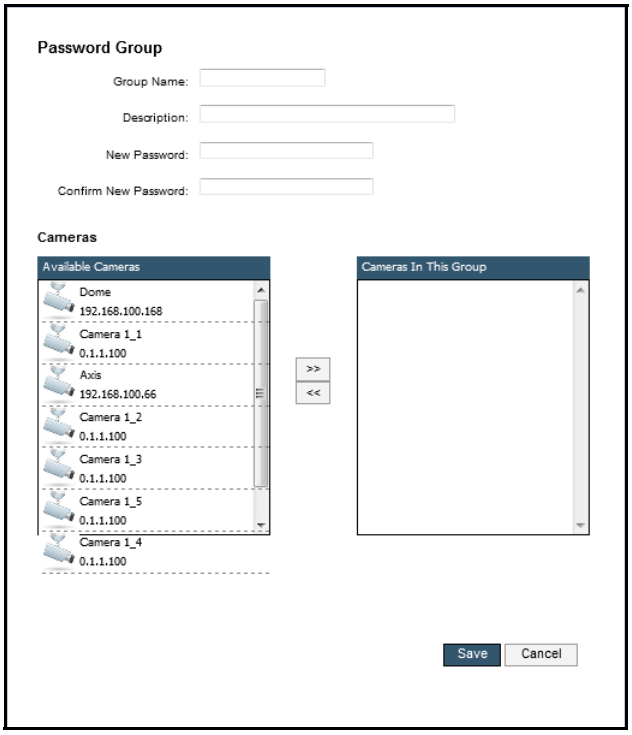
If a password has been changed for a camera or a group of cameras, the NVR is no longer able to communicate with the camera(s). You must create a password group containing the new password and assign the camera(s) with this password to it.

### Procedure 12-1
### Creating a Password Group

| Step | Action |
|---|---|
| **1** | Select **Cameras** from the main menu. |
| **2** | Select **Passwords**.<br>The Passwords page opens (Figure 12-1). |
| **3** | Select **Add New Group**. |

The Password Group window opens.

**Figure 12-1 Password Group Window**




4 Enter a **Group Name**.

5 Enter a **Description**.

6 Enter a **New Password**.

**Note**

This is the password that will now be used by the NVR to connect to the cameras in this password group.

7 Confirm the new password in the **Confirm New Password** field.

8 Select the cameras you want to assign to the password group by dragging the required cameras from the Available Cameras list to the Cameras In this Group List, or by using the >> and << buttons.

9 Click **Save**.

**Note**

If you are editing the password group for a camera attached by an encoder, all cameras connected to the encoder will have the same password. Editing the password group for one camera on an encoder will result in all cameras on that encoder being assigned a new password. A message opens warning that multiple cameras will be updated.

**- End -**

# Delete a Password Group

When you delete a password group, the NVR will try to communicate with the cameras that were in this group, using the manufacturer's default password.

In order for the NVR to successfully communicate with the cameras that were in this group, you must change the password for each camera back to the manufacturers default password, using the direct camera web interface, or reassign the cameras to a new password group.

## Procedure 12-2
## Deleting a Password Group

| Step | Action |
|---|---|
| 1 | Select **Cameras** from the main menu. |
| 2 | Select **Passwords**.<br>The Passwords page opens (Figure 12-1). |
| 3 | Select the checkbox in the password group record that you want to remove. |
| 4 | Click **Remove Group(s)**. |

**- End -**

# Basic System Settings

## Overview

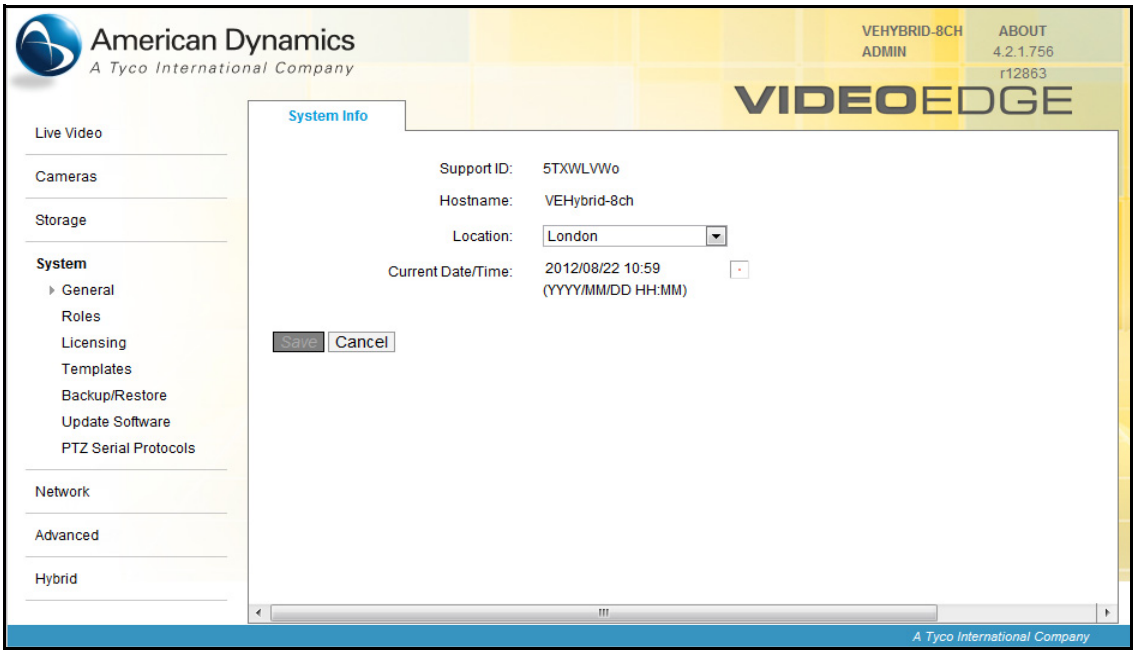
This chapter covers some of the procedures and actions which are carried out using the System Menu and its contained sub menus. The System Menu provides access to the NVR's basic system settings, this allows you to edit details such as its system information, user roles, passwords and software licensing.

In this chapter you will cover how to view and edit the general system settings, and edit the passwords for the Admin and Operator user accounts.

## General System Information

This section details the procedures and actions that can be carried out in the System Info page. This page allows you to edit the hostname, i.e. the name assigned to the NVR, the location, date and time.

Figure 13-1 System Info Page




# Hostname

The Hostname of the NVR can be changed. This provides you the ability to use a bespoke hostname to identify multiple NVRs on a network and in victor client. When the hostname of an NVR is changed it will automatically change in the device list within victor client.

## Procedure 13-1 Editing the Hostname

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **General**.<br>The System Info page opens. |
| 3 | To edit the **Hostname** select the current value. Update the Hostname as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | Click **Save**.<br>A confirmation message displays. |

**- End -**

## Location

The location of the NVR can be defined. A dropdown list provides a list of cities for you to choose from. If the current location of the NVR is not included in the list, it is recommended that you select the nearest city available.

**Note**

When using an NTP Server the location is used to define the time and date as NTP servers use UTC time. For further information refer to Network Settings on page 147.

### Procedure 13-2
### Editing the Location

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **General**.<br>The System Info page opens. |
| 3 | To edit the **Location** select the city of the NVR or nearest city listed from the dropdown list.<br>The dropdown background changes to yellow indicating a change has been made. |
| 4 | Click **Save**.<br>A confirmation message displays. |

**- End -**

## Current Date and Time

The current date and time on an NVR can be manually edited. When using an NTP Server the Time will be synchronised with the server.

**Note**

When using a NTP Server the location is used to define the time and date as NTP servers uses UTC time. For further information refer to Network Settings on page 147.

### Procedure 13-3
### Editing the Current Date and Time

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **General**.<br>The System Info page opens. |

3 To edit the **Current Date** and **Time**, select the current value. Update the Current Date and time as required, enter the date in the field in the following format; **YYYY/MM/DD** for example 2012/01/01.

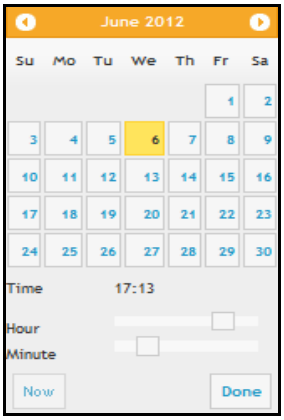
Or

**a** Select the icon.

The Calender opens.

**b** Select the date from the calender.

**Figure 13-2 System Info Calender**




The field background changes to yellow indicating a change has been made.

4 Enter the time in hours and minutes after the date.

You can also use the sliders to adjust the time.

**Note**

Time must be entered in 24 hour format.

5 Click **Save**.

A confirmation message displays.

**- End -**

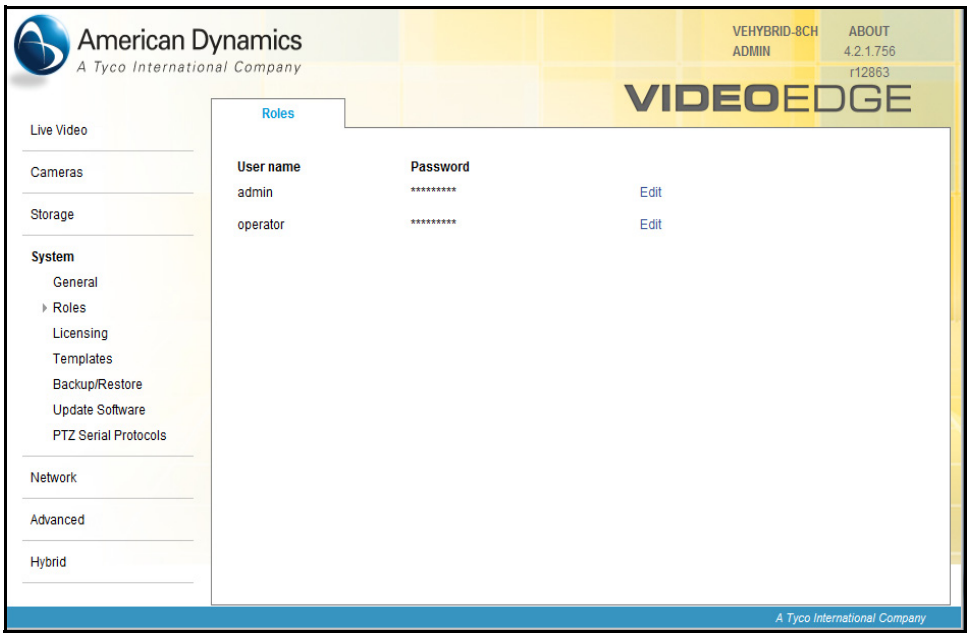
# Roles

This section describes actions that can be carried out using the Roles page. This page allows you to edit the passwords for each of the two user roles i.e. admin and operator.

The admin role is the system administrator role. When logged in as the admin, you will have access to configure all settings in the NVR interface.

If you are logged in as an operator, you will have access to view live video and the current NVR settings but you are not able to make changes.

**Figure 13-3 Roles page**




## Procedure 13-4
## Edit a Password

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Roles**.<br>The Roles page opens. |
| 3 | Select **Edit** beside the User name you want to edit the password for.<br>The password editing fields display. |
| 4 | Enter the current password in the **Current Password** field. |

**Note**

If you are changing from the default password, for the admin role, enter **VIDEO!edge23**, or for the operator role, enter **VideoEdge**.

| | |
|---|---|
| 5 | Enter the new password in the **New Password** field. |

**Note**

It is good practice to choose a password consisting of a combination of upper case letters, lower case letters, numbers and special characters.

| | |
|---|---|
| 6 | Confirm the new password by entering it in the **Confirm Password** text box. |

7 Click **Save**.

**- End -**

# Licensing the NVR

## Overview

During the installation and configuration process of the NVR you will be prompted to licence your NVR. At this stage you can generate a Host ID and apply the licence, alternatively you can continue through the Setup Wizard and use the temporary NVR license.

**Note**

1 The NVR software has a 60-day trial period with a maximum of 128 camera license (16 analytic cameras).

2 If you do not purchase a license by the end of the trial period, the camera and storage functions are automatically disabled.

To apply a licence, use the Licencing page in the NVR web interface (Figure 14-1). From here you can Generate a Host ID, Apply a Licence, edit the Software Service Agreement (SSA) message, add/edit SSA Contacts and add/edit the SMTP Server.

The Licensing Status section provides a summary of the license type, the number of cameras that are licensed on the NVR, the number of cameras with analytics that are licensed on the NVR and the time remaining on the current license.

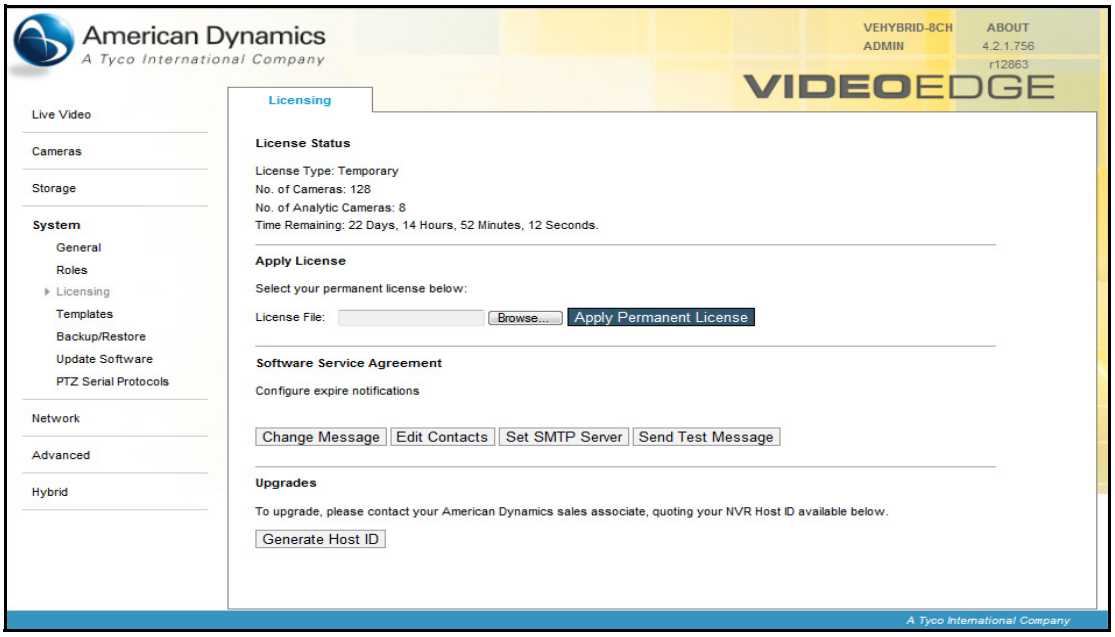
A licence is generated based on the number of devices attached to the NVR. This can be either a camera or a camera encoder with multiple analog cameras attached. A license generated for one NVR cannot be used with another NVR, however, you can replace cameras and devices on the NVR without requiring a license change.

To licence the NVR you must generate a Host ID specific to your NVR and enter the ID on the online registration page. This can be accessed using the VideoEdge Licensing Activation Icon on the NVR Desktop or via the American Dynamics website. Once you receive the licence file you can then apply the permanent licence to your NVR.

The NVR has optional licensable features consisting of:

- Additional cameras (beyond base models)
- Analytics channels

**Figure 14-1 Licensing page**




# Licensing the NVR

This section details the procedures involved in licencing the NVR.

## Generate a Host ID

When it is time to renew your NVR Licence or upgrade your software the Generate Host ID tool is used to generate a Host ID specific to your NVR which should be entered on the VideoEdge 4.2 registration page on the American Dynamics website. The website can be accessed via the VideoEdge Licensing Activation Icon on the NVR Desktop or by going to the following address:

http://www.americandynamics.net/SoftwareRegistration/AutoRegistration/VideoEdgeAutoRegistrationForm.aspx

**Note**

Before you generate the NVR Host ID, you must ensure that all NIC's intended to be used with the NVR, for example, a Client LAN, Camera LANs or a Storage LANs, are already installed on the server.

### Procedure 14-1
### Generate a Host ID

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Licensing**.<br>The Licensing page opens (Figure 14-1). |

3 Click **Generate Host ID** in the **Upgrades** section.

A file download window opens.

4 Click **Open** to view the Host ID. Alternatively you can click **Save** to save the Host ID to your chosen location.

**- End -**

## Apply a Software Licence

After you have received your software licence from the American Dynamics website, you can apply your permanent licence.

### Procedure 14-2
### Applying a License

| Step | Action |
|---|---|
| 1 | Select **System**. |
| 2 | Select **Licensing**.<br>The Licensing page opens (Figure 14-1). |
| 3 | In the **Apply License** section, click **Browse**. |
| 4 | Locate the license file and click **Open**.<br>The filepath is displayed in the **License File** field. |
| 5 | Click **Apply Permanent License**. |

**- End -**

# Software Service Agreement Notifications

The Software Service Agreement (SSA) page allows you to configure a message to alert you when the license is close to expiry. You can add/edit contact email addresses to receive the SSA expiry message and edit the SMTP Server. You can also send a test email message to confirm the settings entered are correct.

**Note**

To be able to use SSA notifications you must ensure that your NVR is configured with a valid Domain Name and Default Gateway. For further information refer to General Network Settings on page 149.

## Edit the SSA Message

You can edit the SSA message that is sent to you when the NVR licence is close to expiry.

### Procedure 14-3
### Edit the SSA Message

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Licensing**.<br>The Licensing page opens (Figure 14-1). |
| 3 | In the **Software Service Agreement** section, click **Change Message**.<br>The SSA Expire Message editing window opens. |
| 4 | To edit the message subject, enter the desired text in the **Subject** field. |
| 5 | To edit the message body, enter the desired text in the **Message** field. |
| 6 | Click **Submit**. |

**- End -**

## Edit SSA Contacts

The SSA contacts, are those who will receive the SSA message to alert them when the NVR licence is about to expire. To receive the message you must add at least one contact's email address to the contacts list. You can add and remove contacts to/from the contact list when required.

### Procedure 14-4
### Edit SSA Contacts

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Licensing**.<br>The Licensing page opens (Figure 14-1). |
| 3 | In the **Software Service Agreement** section, click **Edit Contacts**.<br>The SSA Contacts editing window opens. |
| 4 | To add a contact, enter their email address in the **Add Email** field. |
| 5 | Click **Add**.<br>The email address is added to the contacts list. |
| 6 | (Optional) To add additional contacts to the contacts list repeat Steps 4 and 5. |
| 7 | To remove an email address from the contact list, click **Remove** next to the Email address to be removed.<br>The contacts's email address is no longer in the contacts list. |

**- End -**

## Set the SMTP Server Address

You can set your email SMTP server from the licencing page. There is one SMTP server assigned to the NVR, if you change the server address here, it is the same as changing it through the Email Alerts page.

### Procedure 14-5
### Setting the SMTP Server Address

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Licensing**.<br>The Licensing page opens (Figure 14-1). |
| 3 | In the Software Service Agreement section, click **Set SMTP Server**.<br>The SMTP Server editing window opens. |
| 4 | Enter the IP Address into the **SMTP Server** field. |
| 5 | Click **Submit**. |

**Note**

The SMTP Server address is the same as the address entered in the Email Alerts page, and therefore can also be changed from here.

**- End -**

## Send an SSA Test Message

When you have configured the SSA settings, you can send a test message to the contacts on the SSA contacts list.

### Procedure 14-6
### Sending an SSA Test Message

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Licensing.**<br>The Licensing page opens (Figure 14-1). |
| 3 | Click **Send Test Message** in the **Software Service Agreement** section.<br>A test message is sent to the mailbox of those on the contacts list. |

4 A message opens to confirm if the email has been sent or if it has failed. Click **OK**.

**Note**

If the message has failed to send check your contact's email address(es) and the SMTP server address to confirm they are correct, and re-send.

**- End -**

# Network Settings

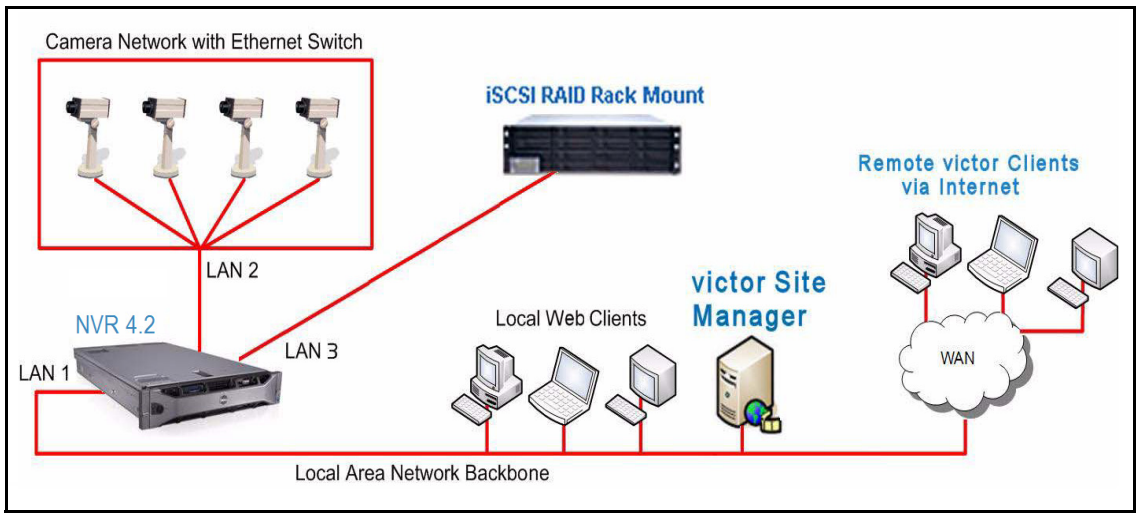
## Overview

This chapter describes the functionality of the NVR Network Menu and its contained sub menus. The Network Menu provides access to the NVR's network settings, this allows you to edit details such as the general network settings, LAN interface settings, DHCP settings, WAN settings and Dynamic Bandwidth.

## Configuring the NVR Network Settings

The design provides the user an extra layer of security for the cameras and reduces the network traffic on the LAN backbone. It also helps prevent accidental or unauthorized changes to the configuration. The example illustrated in Figure 15-1 is only one possible configuration as the NVR can be set up in a number of configurations to meet your bespoke requirements.

**Figure 15-1 Network Diagram Example**




**LAN 1** - Connects the NVR to the network with client PCs. Client PCs typically access the NVR through this port.

**Note**

LAN 1's default IP Address for an NVR supplied as a hardware and software bundle is **10.10.10.10**.

**LAN 2** - Connects the camera network to the NVR. With this architecture, the NVR acts as a firewall between users and the cameras.

The users do not have direct access to the cameras on LAN 2 and must access the NVR in order to view and configure the cameras. As the LAN 2 cameras are not on the main network, they use less network bandwidth from the main network.

In this example DHCP is enabled on LAN 2 so that the NVR can automatically assign IP addresses to cameras that are added to LAN 2. The NVR can have DHCP enabled for each of its NIC's.

**LAN 3** - Connects network storage devices to the NVR.

## Caution

Connecting an NVR running a DHCP server to a network that already has a DHCP server can disrupt network service on that network.

If you have more than one NVR on LAN 2, you will need to disable DHCP on all but one of the LAN 2 NVRs, so that cameras are receiving IP Addresses from only one DHCP server. To disable the DHCP on LAN 2, you will need to log into the NVR, refer to Procedure 15-9 Editing the DHCP Server Settings on page 156Editing the DHCP Server Settings.

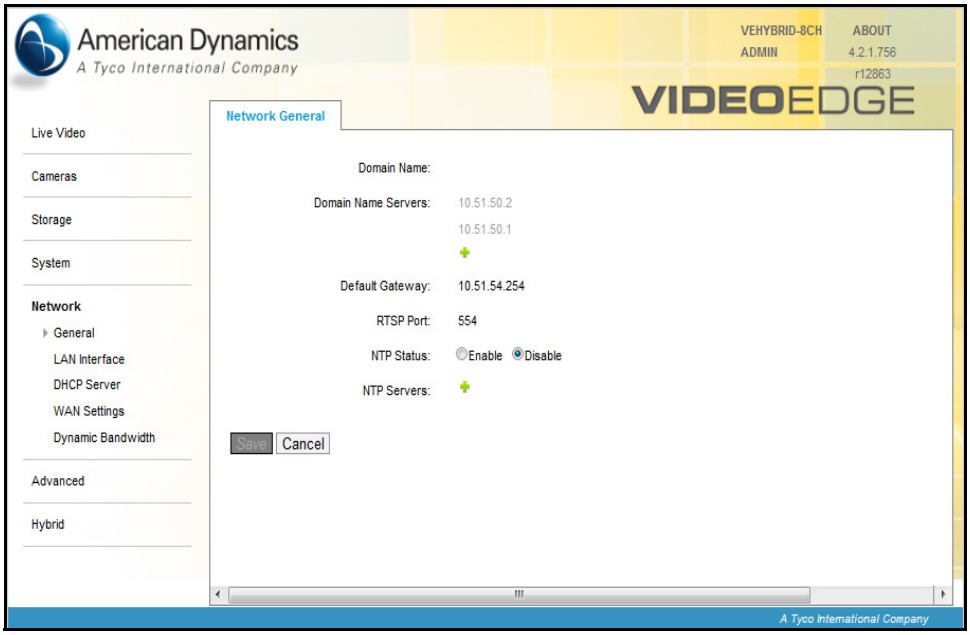
**Note**

When the NVR is supplied as a hardware and software bundle only LAN 1 will be enabled, all other NIC's will be disabled.

# General Network Settings

The General Network page provides you the option to edit the basic connection settings for the NVR network and to enable/disable its NTP functionality. These settings include; Domain Name, Domain Name Servers, Default Gateway, RTSP Port, NTP Status and NTP Servers.

**Figure 15-2 General Network Page**




## Domain Name and Domain Name Servers

Under the General Network settings you can assign a bespoke Domain Name and create a list of DNS servers which provide name resolution services i.e. convert hostnames to IP addresses.

### Procedure 15-1
### Edit the Domain Name and Domain Name Servers

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **General**.<br>The General Network settings page opens. |
| 3 | To edit the **Domain Name** select the current value. Update the Domain Name as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | To add a Domain Name Server to the Domain Name Servers select the icon.<br>A text box displays. |
| 5 | Enter the **IP Address** in the field.<br>The field background changes to yellow indicating a change has been made. |
| 6 | To enter several Domain Server IP Addresses select the icon to add an additional IP Address field and enter the IP Address. |

7 Click **Save**.

Confirmation messages display.

**- End -**

## Default Gateway

In the General Network settings you can edit the IP Address of the Default Gateway. The default gateway must be set manually if the NVR is not using a DHCP server. The default gateway allows the NVR to have connectivity with IP addresses beyond the directly connected subnets of its own NICs.

### Procedure 15-2
### Editing the Default Gateway

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **General**.<br>The General Network settings page opens. |
| 3 | To edit the **Default Gateway** select the current value. Update the Default Gateway as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | Click **Save**. A warning dialog will display stating ‘Changing the default gateway may result in your NVR becoming inaccessible. If this happens, you will need to physically connect to the NVR to re-enable network access. Are you sure you want to proceed?’. |
| 5 | Click **OK**.<br>A confirmation message displays. |

**- End -**

## RTSP Port

If you need to modify the default RTSP Streaming Port for your NVR to conform to your network rules, you can use the RTSP Streaming Port field on the General Settings page to change the port setting.

### Procedure 15-3
### Editing the RTSP Port

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **General**.<br>The General Network settings page opens. |

3 To edit the **RTSP Port** select the current value. Update the RTSP Port as required.

The field background changes to yellow indicating a change has been made.

4 Click **Save**.

A confirmation message displays.

**Note**

The default RSTP Port number is **554**.

**- End -**

## NTP Status and NTP Servers

The NVR can be used as a Network Time Protocol (NTP) Server to all reachable network devices. In this configuration it will accept and respond to NTP requests from all accessible networks.

**Note**

Setting the NVR to use NTP can affect the time and date settings of cameras and other devices with access to the same networks as the server if you configure these devices to use the NVR as an NTP server. The NTP server will not affect other Windows devices on the LAN with the NVR.

Alternatively you can use external NTP servers to synchronize date and time instead of using the NVR as the NTP Server.

**Note**

You should setup all NVRs and client systems to use the same NTP Server, to synchronize date and time settings.

### Procedure 15-4
### Editing the NTP Status to use NVR as a NTP Server

**Step Action**

1 Select **Network**.

2 Select **General**.

The General Network settings page opens.

3 To edit the NTP Status click either the **Enable** or **Disable** option buttons.

The area behind the option buttons changes to yellow indicating a change has been made.

4 Click **Save**.

A confirmation message displays.

**- End -**

### Procedure 15-5
### Editing the NTP Status and NTP Servers to Synchronize Date and Time from the Internet

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **General**.<br>The General Network settings page opens. |
| 3 | To edit the NTP Status click either the **Enable** or **Disable** option buttons.<br>The area behind the option buttons changes to yellow indicating a change has been made. |
| 4 | To edit the **NTP Servers** click the icon. |
| 5 | Enter the NTP Server IP Address in the field.<br>The field background changes to yellow indicating a change has been made. |
| 6 | To enter several NTP Server IP Addresses click the icon to add an additional IP Address. Enter the IP Address in the field. |
| 7 | Click **Save**.<br>A confirmation message displays. |

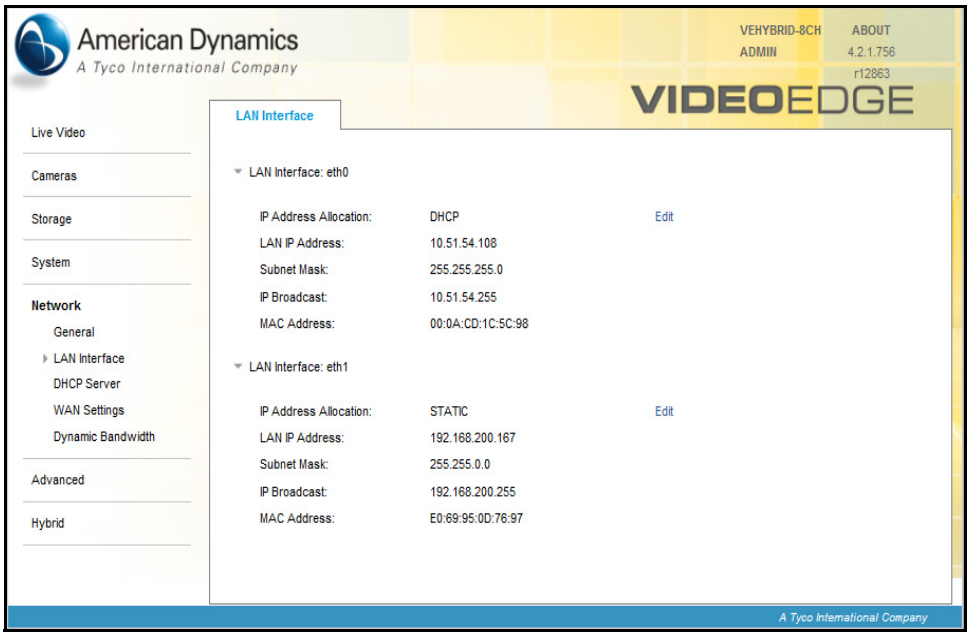
**- End -**

# LAN Interface Settings

The LAN Interface page allows you to enable and disable the NICs of the NVR. Each NIC provides a LAN interface for the NVR.

The LAN Interface page also allows you to edit the available LAN Interfaces. In the LAN Interface page the NIC's associated with the NVR will be displayed and available for editing. The LAN Interface page allows you to edit the IP Address Allocation, LAN IP Address, Subnet Mask and IP Broadcast Address. The page will also display the MAC address for each NIC on the NVR.

**Figure 15-3 LAN Interface Page**




## Procedure 15-6
## Enabling NIC's

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **LAN Interface**.<br>The LAN Interface page opens. |
| 3 | Select the dropdown arrow next to the LAN Interface you wish to edit. |
| 4 | Select **Edit**. |
| 5 | Select the **IP Address Allocation** dropdown. |
| 6 | Select **DHCP**, this will allow a DHCP Server on the LAN to assign an IP address for that NIC of the NVR. |

**Note**

The use of DHCP for all of the NVR's NICs is not recommended. To open the NVR Web Interface the IP address of one of the NICs must be known, if all the IP addresses are dynamic they will vary in value. It is recommended that a NIC is configured with a static IP address and subnet mask for this reason.

Or

Select **STATIC** to permanently assign an IP address, subnet mask and IP broadcast to the NVR.

When using Static IP addresses you will be required to enter the IP address, subnet mask and IP broadcast in the corresponding fields. Refer to Procedure 15-8 Editing the LAN Interface Values on page 154.

7 Click **Save**.
A dialog box displays advising that changing network interface settings may result in your NVR becoming inaccessible.

8 Click **OK**.

**- End -**

## Procedure 15-7
## Disabling NIC's

| Step | Action |
|---|---|

1 Select **Network**.

2 Select **LAN Interface**.

The LAN Interface page opens.

3 Select the dropdown arrow next to the LAN Interface you wish to edit.

4 Select **Edit**.

5 Select the **IP Address Allocation** dropdown.

6 Select **NONE**.

When **NONE** is selected the LAN Interface options for that NIC will collapse leaving only the IP Address Allocation displayed.

7 Click **Save**.

A dialog box displays advising that changing network interface settings may result in your NVR becoming inaccessible.

8 Click **OK**.

**Note**

If you disable eth0 using the NVR Web Interface it will terminate its connection on that NIC. To re-establish connection you can access the Web Interface using the IP Address of one of the other active NIC's. Alternatively you can log into the NVR's Linux OS to edit the network settings, refer to Appendix D: NVR Troubleshooting on page 261.

**- End -**

## Procedure 15-8
## Editing the LAN Interface Values

| Step | Action |
|---|---|

1 Select **Network**.

2 Select **LAN Interface**.

The LAN Interface page opens.

3 Select the dropdown arrow next to the LAN Interface you wish to edit.

4 Select **Edit**.

5 To edit the **LAN IP Address**, enter the desired IP Address in the field.

6 To edit the **Subnet Mask**, enter the desired Subnet Mask in the field.

7 To edit the **IP Broadcast Address**, enter the desired Broadcast Address in the field.

8 Click **Save**.

**Note**

The displayed MAC Address cannot be edited.

**- End -**

## DHCP Server Settings

The DHCP Server page provides the option to configure the NVR to host a DHCP Server for each network card plugged into the system. This allows the NVR to allocate IP addresses from the range specified when other devices request IP allocation.

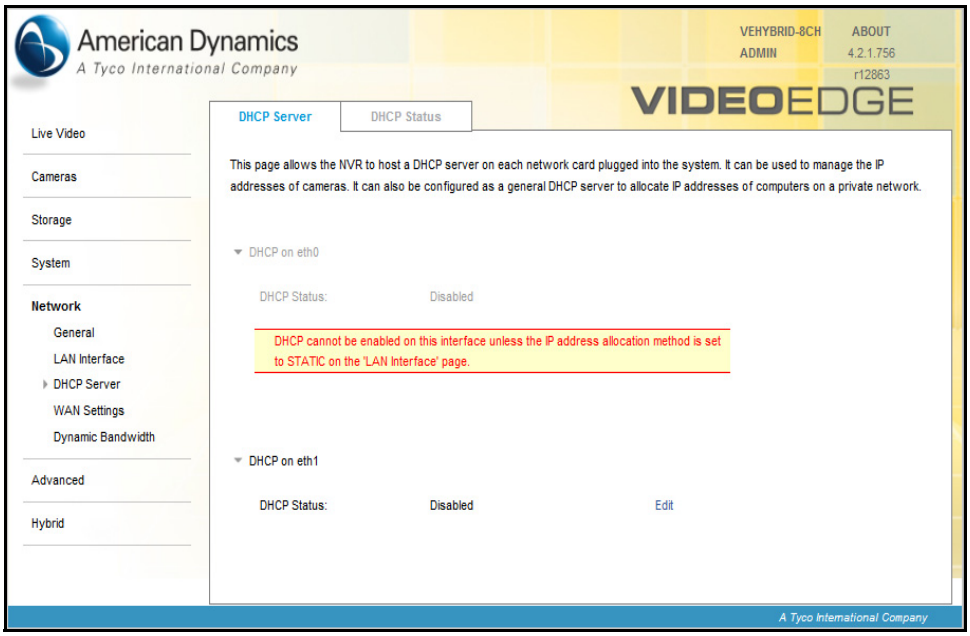
The page allows you to edit the DHCP Status and the Start and End Range of IP Addresses to be included during automatic searching for IP Devices.

The DHCP Status page allows you to view all active devices which have been assigned an IP address by the NVR acting as a DHCP server. The page displays the IP addresses in use by the device, its MAC address, when it was last active and the device's hostname.

### Caution

You should only set up the NVR as a DHCP Server if you are positive the LAN does not already have a DHCP Server, and the NVR has been assigned a static IP Address. Otherwise you could have two different DHCP Servers giving out IP addresses, and this could cause network problems.

**Figure 15-4 DHCP Server Page**




## Procedure 15-9
## Editing the DHCP Server Settings

| Step | Action |
|---|---|

**1** Select **Network**.

**2** Select **DHCP Server**.

The DHCP Server settings page opens.

**3** Select the dropdown arrow next to the LAN Interface you wish to edit.

**Note**

NICs which have been configured with a DHCP IP Address Allocation will be greyed out and not available to be used to host DHCP Servers. A message is also displayed stating ‘DHCP cannot be enabled on this interface unless the IP allocation method is set to STATIC on the ‘LAN Interface’ page.’

**4** Select **Edit**.

**5** To edit the DHCP Status select either the **Enable** or **Disable** option buttons**.**

When **Enabled** is selected the DHCP options for that NIC expand.

**6** To edit the DHCP Start Range and End range type the lowest and highest IP address to be assigned, respectively. For example, if your network addresses were between 10.11.12.50 and 10.11.12.100, you could type 10.11.12.50 for DHCP Range Start and 10.11.12.100 for DHCP Range End.

7 Click **Save**.

**Note**

Subnet and Netmask can not be edited in this page. The DHCP Start Range and End Range can only be entered when the DHCP Status is set to **Enabled**.

**- End -**

### Procedure 15-10
### Viewing the DHCP Status

| Step | Action |
|---|---|

1 Select **Network.**

2 Select **DHCP Server**.

The DHCP Server settings page opens.

3 Select the **DHCP Status** page.

The DHCP Status page opens.

**Note**

You can now view all devices being managed by the NVR's DHCP server. The information displayed includes the IP addresses in use by the device, MAC address for connected devices, the time a device was last active and the Hostname for each device.

**- End -**

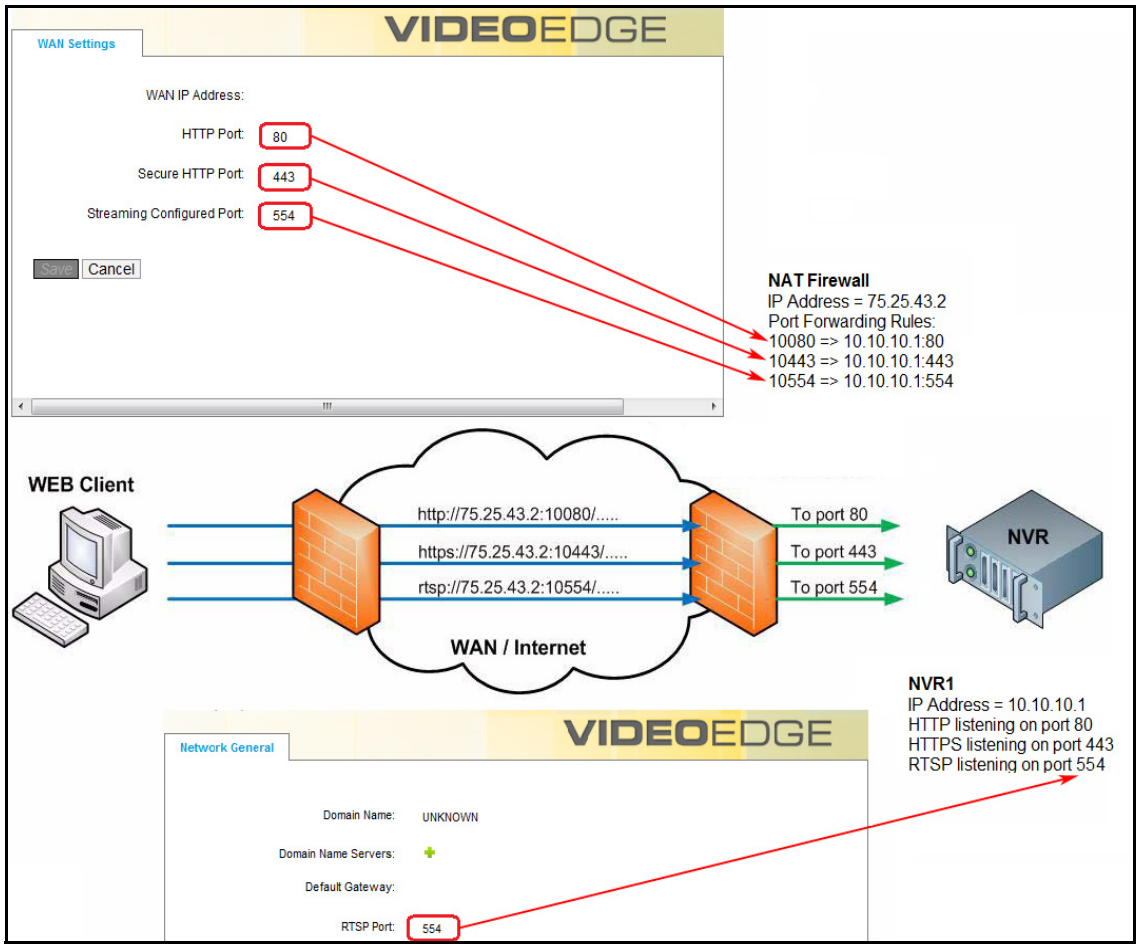
# WAN Settings

The WAN Settings page allows you to configure the NVR to operate in a wide area network (WAN) configuration. The WAN Settings page lets you specify the name or IP address that can be used to access an NVR located behind a NAT firewall (such as a corporate LAN) that presents a single public address for connections from outside the LAN. You can also specify the ports that are used for HTTP, secure HTTP and streaming (RTSP) connections to the NVR. You can also enter a list of allowed IP addresses. In addition, the General Settings page allows you to change the RTSP Streaming Port, refer to Procedure 15-3 Editing the RTSP Port on page 150.

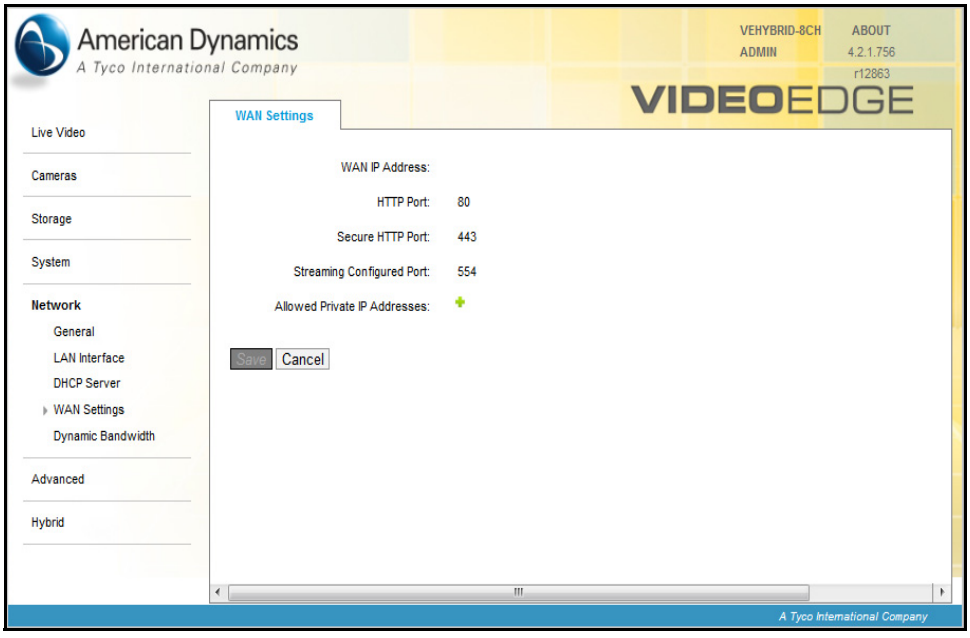
**Note**

For a new install, the Setup WAN fields display the default values. If you upgrade the NVR, these fields will display the previously assigned values however if you carry out an appliance install the values will be lost unless a template has been created and applied, refer to NVR Failover, Configuration Backup, Templates and Updates on page 177. If you enter a value into any of these fields, that value is saved, and is displayed until modified.

## Figure 15-5 WAN Port Mapping Exam




## Figure 15-6 WAN Settings Page



## WAN IP Address

Under the WAN Settings you can edit the WAN IP Address.

### Procedure 15-11
### Editing the WAN IP Address

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **WAN Settings**.<br>The WAN settings page opens. |
| 3 | To edit the **WAN IP Address** select the current value. Update the WAN IP Address as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | Click **Save**.<br>A confirmation message displays. |

**- End -**

## HTTP Port

This is the port number used to identify this NVR if more than one NVR is behind the NAT firewall.

In the HTTP address typed by the user when accessing an NVR, a port number can be specified (for example, http://70.30.22.81:80. Port 80 is normally assumed by default. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by port forwarding rules at the firewall level. This means that both NVRs will still listen on port 80 for HTTP requests but that publicly NVR1 might be contactable as http://70.30.22.81:80, while NVR2 is contactable as http://70.30.22.81:10080. The firewall is configured to accept NVR2 requests at http://70.30.22.81:10080 and forward them to http://<NVR2 private IP>:80.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10080.

### Procedure 15-12
### Editing the HTTP Port

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **WAN Settings**.<br>The WAN settings page opens. |
| 3 | To edit the **HTTP Port** select the current value. Update the HTTP Port as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | Click **Save**. |

A confirmation message displays.

**Note**

The default HTTP Port value is **80**.

**- End -**

## Secure HTTP Port

This is the port number used to identify this NVR if more than one NVR is behind the NAT firewall, and a secure connection (https) is being made.

If an HTTPS address is being used to access an NVR, a port number can be specified (for example, https://70.30.22.81:443. Port 443 is normally assumed by default. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by port forwarding rules at the firewall level. This means that both NVRs will still listen on port 443 for HTTPS requests but that publicly NVR1 might be contactable as https://70.30.22.81:443, while NVR2 is contactable as https://70.30.22.81:100443. The firewall is configured to accept NVR2 requests at https://70.30.22.81:100443 and forward them to https://<NVR2 private IP>:443.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10443.

### Procedure 15-13
### Editing the Secure HTTP Port

| Step | Action |
|---|---|
| **1** | Select **Network**. |
| **2** | Select **WAN Settings**.<br>The WAN settings page opens. |
| **3** | To edit the **Secure HTTP Port** select the current value. Update the Secure HTTP Port as required.<br>The field background changes to yellow indicating a change has been made. |
| **4** | Click **Save**.<br>A confirmation message displays. |

**Note**

The default HTTP Port value is **443**.

**- End -**

## Streaming Configured Port

This is the port number used for the real time streaming protocol (RTSP) connection to this NVR if more than one NVR is behind the NAT firewall, when video is being streamed to a client programmatically via RTSP.

Port 554 is the default port for RTSP connection. However, if two NVRs are behind the same NAT firewall, they are both exposed as the same public address, so the only way to distinguish between them is by setting up port forwarding rules at the firewall level. This means that both NVRs listen on port 554 for HTTPS requests but that publicly NVR1 might be contactable as https://70.30.22.81:554, while NVR2 is contactable as https://70.30.22.81:100554. The firewall is configured to accept NVR2 requests at https://70.30.22.81:100554 and forward them to https://<NVR2 private IP>:554.

This field must be set in scenarios where multiple NVRs are situated behind the same NAT firewall. In this example, this field on NVR2 must be set to 10554.

### Procedure 15-14
### Editing the Streaming Configured Port

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **WAN Settings**.<br>The WAN settings page opens. |
| 3 | To edit the **Streaming Configured Port** select the current value. Update the Streaming Configured Port as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | Click **Save**.<br>A confirmation message displays.<br>**Note**<br>The default HTTP Port value is **554** |

**- End -**

## Allowed IP Addresses

These are the public IP addresses that are permitted for use with the NVR. A public IP address is one which is not in the following ranges:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

### Procedure 15-15
### Adding Allowed IP Addresses

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **WAN Settings**.<br>The WAN Settings page opens. |
| 3 | To add an IP Address to the Allowed IP Address select the icon.<br>The IP Address and Subnet Mask text boxes display.<br>The NIC dropdown displays. |
| 4 | Enter the IP address in the **IP Address** field. |
| 5 | Enter the subnet mask in the **Subnet Mask** field. |
| 6 | Select the desired NIC from the **NIC** dropdown. |
| 7 | Click **Save**. |

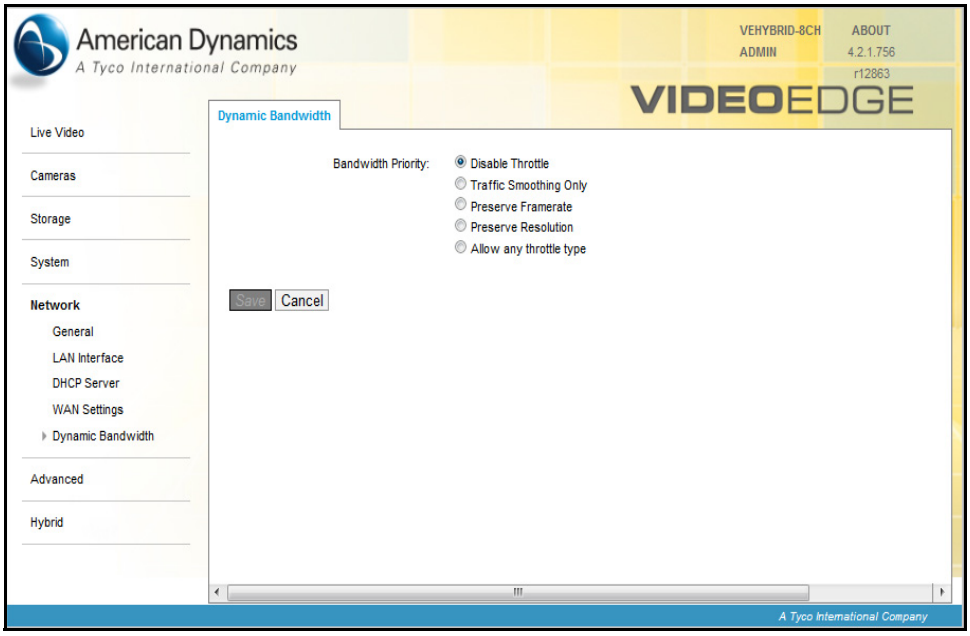
**- End -**

# Dynamic Bandwidth

In the Dynamic Bandwidth page you can edit the Bandwidth throttling, by default the Bandwidth throttling is disabled (no framedropping or transcoding are invoked). Editing Bandwidth Throttling changes the type of throttling which is utilized during streaming of video.

The options available for configuration on the page vary with the Bandwidth Priority which is selected. Options will only display for editing if they are applicable to that Bandwidth Priority.

**Figure 15-7 Dynamic Bandwidth Page**




## Bandwidth Priority

Bandwidth Priority allows you to select the type of throttling you wish to attempt to use. You can chose to disable throttling or use one of the four predefined throttling options; **Traffic Smoothing Only**, **Preserve Framerate**, **Preserve Resolution** and **Allow any throttle type**.

When any of the four predefined throttling types are selected the **Traffic Smoothing** fields display. Traffic Smoothing reduces the appearance of framedrop on the LAN client by smoothing traffic from the NVR. Traffic Smoothing can be configured for both the client and the stream, it is entered in Mbps and its default values for each of the four predefined bandwidth priorities will appear as 300 Mbps for the client and 75 Mbps for the stream, these figures can be edited to match the capabilities of your network and your client host (client NIC and performance), as this feature addresses issues with poor performance network cards on victor client.

When Preserve Framerate, Preserve Resolution and Allow any throttle type are selected the WAN and LAN bitrate cap dropdowns display.

**Note**

A bitrate cap limits the amount of streaming data (i.e. video) leaving the NVR to remote clients or clients connected using VPN. The WAN bitrate cap cannot exceed the LAN bitrate cap.

The dropdown menus provide a list of predefined values which you can choose from. Alternatively a custom value can be entered and there is no minimum entry value. This allows experienced users to customise their WAN and LAN Bitrate Caps to best utilise their networks capabilities.

**Note**

If the LAN or WAN bitrate cap is set to a value which is less than the Traffic Smoothing value, Traffic Smoothing will have no affect on the transmitted stream as it will adhere primarily to the bitrate cap. It is recommended that Traffic Smoothing is set to a value less than or equal to the LAN and WAN bitrate caps.

Usually WAN connections have lower bandwidth than LAN connections, if the WAN bandwidth is less than the default value of 150 Mbps Traffic Smoothing will have little to no effect.

When Preserve Framerate and Allow any throttle type are selected the Transcode Limit dropdown also displays. This allows you to limit the number of transcoded streams between 1 and 4 to best suit your CPU's capabilities.

## Traffic Smoothing Only

Allows the ability to pace the traffic leaving the NVR to individual clients without incurring framedrop or transcode. This smooths bursts of traffic which may cause issues for some consumer grade NICs consuming this data.

### Procedure 15-16
### Selecting Traffic Smoothing Only

| Step | Action |
|---|---|

1 Select **Network**.

2 Select **Dynamic Bandwidth**.

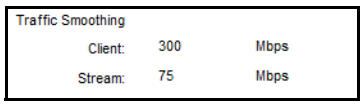
The Dynamic Bandwidth page opens.

3 Click the **Traffic Smoothing Only** option button.

The area behind the option buttons changes to yellow indicating a change has been made.

The Traffic Smoothing fields display.

**Figure 15-8 Traffic Smoothing Fields**




4 To edit the **Client** and **Stream** fields select the current values. Update the Client and Stream values as required.

The field backgrounds change to yellow indicating a change has been made.

5 Click **Save**.

Confirmation messages display.

**- End -**

## Preserve Framerate

Any overloaded network or set caps on the NVR/client will allow the NVR to adapt the streams accordingly by reducing the bitrate by transcoding a stream to H.264, lower bitrate and possibly lower resolution. If all transcode resources are used, best effort streaming will occur.

### Procedure 15-17
### Selecting Preserve Framerate

| Step | Action |
|---|---|

**1** Select **Network**.

**2** Select **Dynamic Bandwidth**.

The Dynamic Bandwidth page opens.

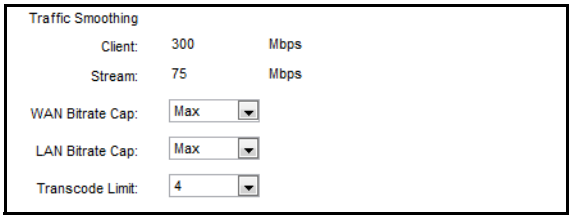
**3** Click the **Preserve Framerate** option button.

The area behind the option buttons changes to yellow indicating a change has been made.

The Traffic Smoothing fields display.The LAN and WAN Bitrate Cap dropdowns display.

The Transcode Limit Dropdown displays.

**Figure 15-9 Traffic Smoothing, WAN and LAN Bitrate Caps and Transcode Limit**




**4** To edit the **Client** and **Stream** fields select the current values. Update the Client and Stream values as required.

The field backgrounds change to yellow indicating a change has been made.

**5** The WAN and LAN Bitrate Caps can be set to either a predefined value from the dropdown menus or alternatively a custom value can be entered in the field.

To use a predefined value open the dropdown, select the desired predefined value from the list.

Or

**a** To use a custom value, select **Custom** from the dropdown.
The custom entry field displays.

**b** To edit the **bitrate cap** value select the current value. Update the bitrate cap value as required.

The field backgrounds change to yellow indicating a change has been made.

**Note**

The custom value must be entered in **kbps**. For example to enter a value of 5.5Mbps you would type a value of 5500.

6 From the **Transcode Limit** dropdown select the number of streams desired.

7 Click **Save**.

Confirmation messages display.

**- End -**

## Preserve Resolution

Any overloaded network or set caps on the NVR/client will allow the NVR to adapt the streams accordingly by reducing the stream output using framedrop. If framedrop should fail or doesn't occur, then best effort streaming will occur.

### Procedure 15-18
### Selecting Preserve Resolution

| Step | Action |
|---|---|

1 Select **Network**.

2 Select **Dynamic Bandwidth**.

The Dynamic Bandwidth page opens.

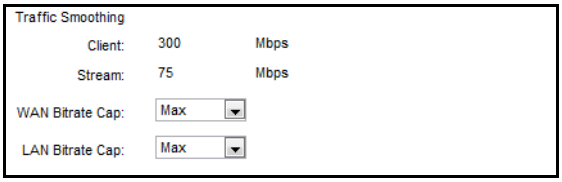
3 Click the **Preserve Resolution** option button.

The area behind the option buttons changes to yellow indicating a change has been made.

The Traffic Smoothing fields display.

The LAN and WAN Bitrate Cap dropdowns display.

**Figure 15-10 Traffic Smoothing, LAN and WAN Bitrate Caps**




4 To edit the **Client** and **Stream** fields select the current values. Update the Client and Stream values as required.

The field backgrounds change to yellow indicating a change has been made.

5 The WAN and LAN Bitrate Caps can be set to either a predefined value from the dropdown menus or alternatively a custom value can be entered in the field.

To use a predefined value open the dropdown, select the desired predefined value from the list.

Or

**a** To use a custom value, select **Custom** from the dropdown.
The custom entry field displays.

**b** To edit the **bitrate cap** value select the current value. Update the bitrate cap value as required.

The field backgrounds change to yellow indicating a change has been made.

**Note**

The custom value must be entered in **kbps**. For example to enter a value of 5.5Mbps you would type a value of 5500.

6 Click **Save**.

Confirmation messages display.

**- End -**

## Allow Any Throttle Type

Any overloaded network or set caps on the NVR/client will allow the NVR to adapt the streams accordingly by either transcoding, transcoding and framedropping on the transcoded stream and if all the transcode resources are used, framedrop will be invoked only. If any of the above should fail, then best effort streaming will occur.

### Procedure 15-19
### Selecting Allow Any Throttle Type

| Step | Action |
|---|---|

1 Select **Network**.

2 Select **Dynamic Bandwidth**.

The Dynamic Bandwidth page opens.

3 Click the **Allow any throttle type** option button.

The area behind the option buttons changes to yellow indicating a change has been made.

The Traffic Smoothing fields display.

The LAN and WAN Bitrate Cap dropdowns display.

The Transcode Limit Dropdown displays.

4 To edit the **Client** and **Stream** fields select the current values. Update the Client and Stream values as required.

The field backgrounds change to yellow indicating a change has been made.

5 The WAN and LAN Bitrate Caps can be set to either a predefined value from the dropdown menus or alternatively a custom value can be entered in the field.

To use a predefined value open the dropdown, select the desired predefined value from the list.

Or

**a** To use a custom value, select **Custom** from the dropdown.
The custom entry field displays.

**b** To edit the **bitrate cap** value select the current values. Update the bitrate cap value as required.

The field backgrounds change to yellow indicating a change has been made.

**Note**

The custom value must be entered in **kbps**. For example to enter a value of 5.5Mbps you would type a value of 5500.

6 From the **Transcode Limit** dropdown select the number of streams desired.

7 Click **Save**.

Confirmation messages display.

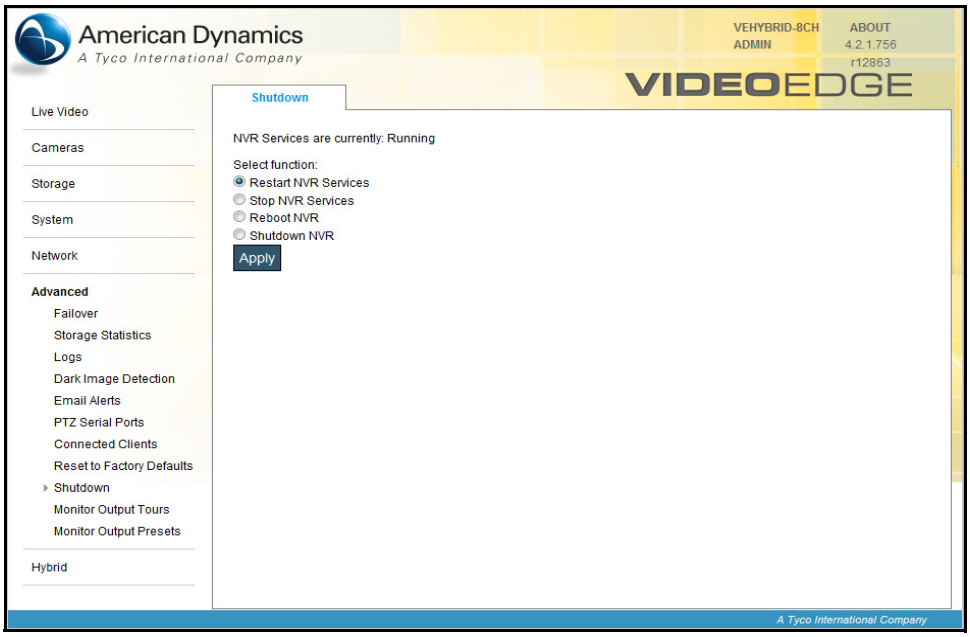
**- End -**

# System Shutdown and Reset Factory Defaults

## Overview

This chapter describes how to use the system shutdown functions of the NVR and how to reset the NVR to factory default settings. The Shutdown page allows you to Restart the NVR Services, Stop NVR Services, Reboot the NVR and Shutdown the NVR.

**Figure 16-1 Shutdown Page**




## Restart NVR Services

The Shutdown page allows you to restart the NVR services, this will restart the NVR software such as recording and playback services, however it will not restart the operating system. Restarting NVR services is faster than rebooting the NVR.

### Procedure 16-1
### Restart NVR Services

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Shutdown**.<br>The Shutdown page opens. |
| 3 | Select **Restart NVR Services** option button. |
| 4 | Click **Apply**. |

**- End -**

## Stop NVR Services

NVR Services can be stopped permanently. By stopping NVR services you can release resources and maximise system performance of some SUSE features.

**Note**

It is highly recommended that you stop NVR Services before configuring storage.

### Procedure 16-2
### Stop NVR Services

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Shutdown**.<br>The Shutdown page opens. |
| 3 | Select **Stop NVR Services** option button. |
| 4 | Click **Apply**.<br>A message box opens, “This will stop NVR Services. Are you sure you want to continue?” |
| 5 | Click **Yes**. |

The confirmation message, “NVR Services have stopped - The NVR will not record or display live media until the services are restarted” displays and the NVR services are disabled.”

**Note**

When you have stopped NVR services, use the Restart NVR Services option (Procedure 16-1 Restart NVR Services) to restart the services.

**- End -**

# Reboot the NVR

The Shutdown page allows you to reboot the NVR, this will cause the NVR to go through a soft reboot when applied.

## Procedure 16-3
## Reboot the NVR

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Shutdown**.<br>The Shutdown page opens. |
| 3 | Select **Reboot NVR** option button. |
| 4 | Click **Apply**. |

**- End -**

# Shutdown the NVR

The Shutdown page allows you to shutdown the NVR, this will cause the NVR to fully power down when applied.

## Procedure 16-4
## Shutdown the NVR

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Shutdown**.<br>The Shutdown page opens. |

3 Select **Shutdown NVR** option button.

4 Click **Apply**.

**Note**

To restart the NVR after it has been shut down it must be manually turned on at the server.

**- End -**

# Reset Factory Defaults

The Reset Factory Defaults functionality allows you to revert several of the NVR's characteristics back to their default settings it will however not implement any changes to the servers Linux Operating System. During a Reset Factory Defaults function the recorder will not be able to record or display live video until the process is complete.

Once the Reset Factory Defaults is complete you will have to reconfigure the NVR using the Setup Wizard.

The following settings will be affected when carrying out a Reset Factory Defaults function:

- **Storage** settings, configured using the NVR web interface will be erased.
- **Failover** settings, if configured will be erased.
- **User Passwords** for all user roles will be reset to the factory defaults, refer to Roles on page 138 for more information on default user roles and passwords.
- **Alarm** settings, if configured will be erased.
- **Saved Media files (video/audio)**, the NVR supports several options for keeping or deleting the Saved Media files, they are as follows:
    - **Reset to Factory Defaults AND Erase All Media** - This will delete **all** your recorded media (video/audio, protected media and video analytic data). Choose this option if you want to remove all media and fully restore to factory defaults.
    - **Reset to Factory Defaults AND Keep Media** - This will preserve all your recorded media. Choose this option for a quick reset of NVR settings but preserve all media and databases.

**Note**

This option will keep both the media and the current media database. If there are continuing issues a reset with full media re-indexing is recommended.

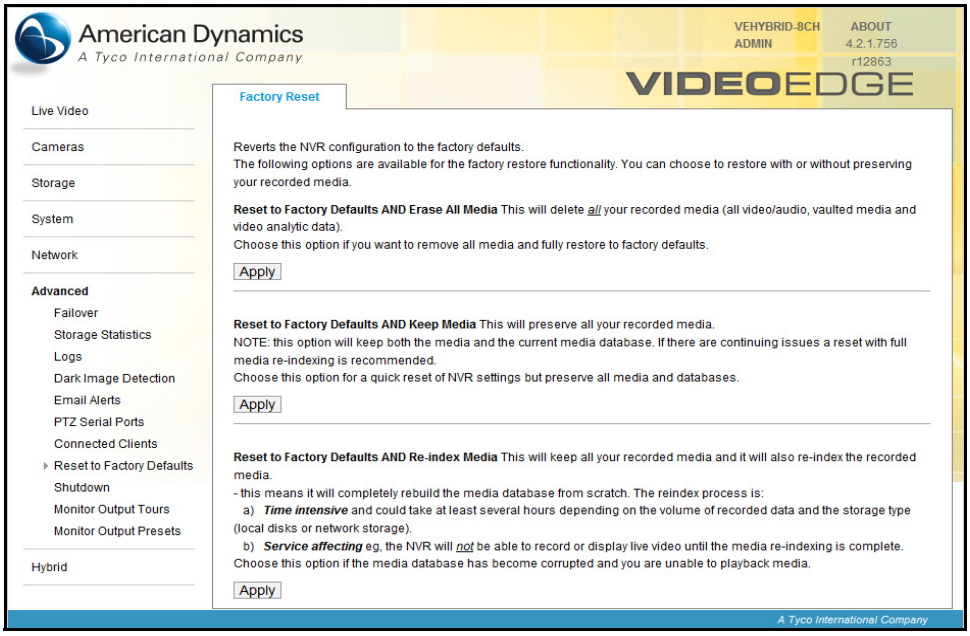
- **Reset to Factory Defaults AND Re-index Media** - This will keep all your recorded media and it will also re-index the recorded media. The media

database will be completely rebuilt during this process. Choose this option if the media database has become corrupt and you are unable to playback media.

**Note**

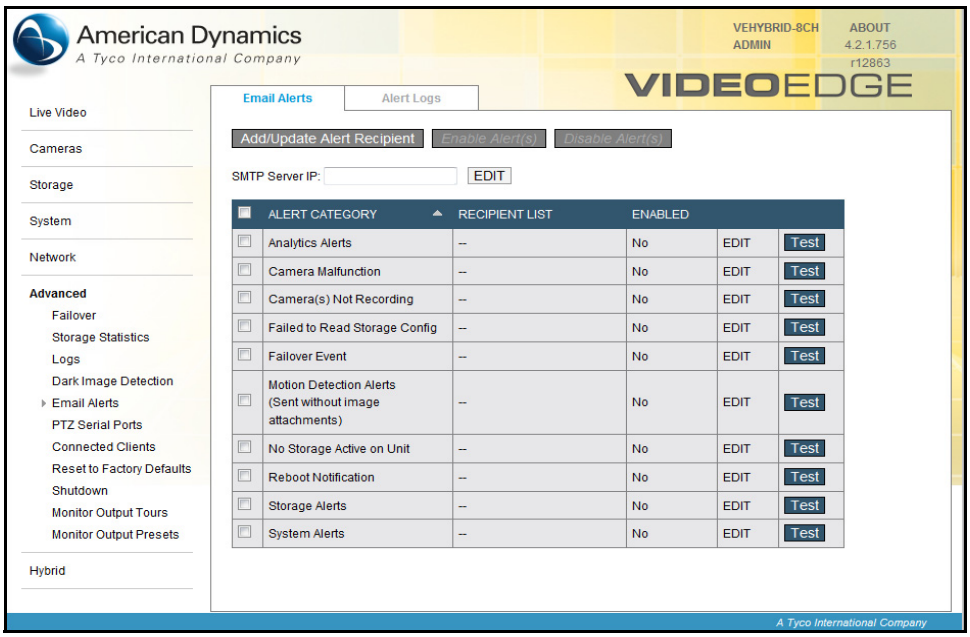
The re-index process is time intensive and can take several hours to complete depending on the volume of recorded data and the storage type (local disks or network storage). The NVR will not be able to record or display live video until the media re-indexing is complete.

**Figure 16-2 Factory Reset Page**


American Dynamics
A Tyco International Company
VEHYBRID-8CH
ADMIN
ABOUT
4.2.1.756
r12863
VIDEOEDGE
Live Video
Cameras
Storage
System
Network
Advanced
Failover
Storage Statistics
Logs
Dark Image Detection
Email Alerts
PTZ Serial Ports
Connected Clients
Reset to Factory Defaults
Shutdown
Monitor Output Tours
Monitor Output Presets
Hybrid
Factory Reset
Reverts the NVR configuration to the factory defaults.
The following options are available for the factory restore functionality. You can choose to restore with or without preserving your recorded media.
Reset to Factory Defaults AND Erase All Media This will delete all your recorded media (all video/audio, vaulted media and video analytic data).
Choose this option if you want to remove all media and fully restore to factory defaults.
Apply
Reset to Factory Defaults AND Keep Media This will preserve all your recorded media.
NOTE: this option will keep both the media and the current media database. If there are continuing issues a reset with full media re-indexing is recommended.
Choose this option for a quick reset of NVR settings but preserve all media and databases.
Apply
Reset to Factory Defaults AND Re-index Media This will keep all your recorded media and it will also re-index the recorded media.
- this means it will completely rebuild the media database from scratch. The reindex process is:
a) Time intensive and could take at least several hours depending on the volume of recorded data and the storage type (local disks or network storage).
b) Service affecting eg, the NVR will not be able to record or display live video until the media re-indexing is complete.
Choose this option if the media database has become corrupted and you are unable to playback media.
Apply
A Tyco International Company

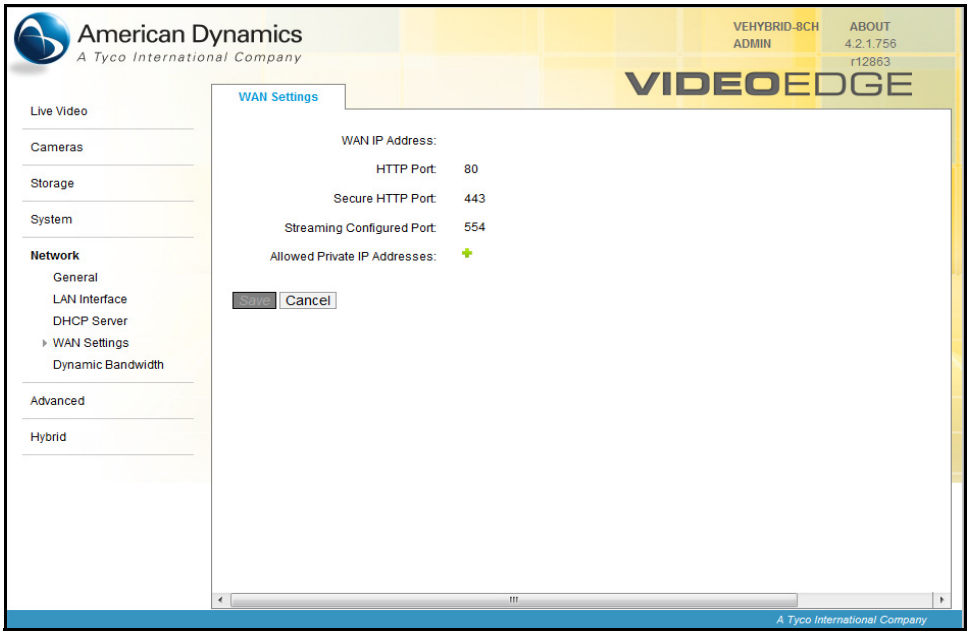
- **Email Alerts** will all be disabled and any email addresses entered for alert notifications will be erased. The SMTP Server address will also be erased.

**Figure 16-3 Email Alerts Page After Reset**




- **WAN Settings** will be reset to factory defaults.

**Figure 16-4 WAN Settings After Reset**




- **Cameras** will be erased leaving the camera list empty.

**Note**

Settings linked to the OS will not be affected. These include Network Settings, Services (eg. NTP, DHCP and so on) and the System Settings. The NVR License will also not be affected.

## Procedure 16-5
## Reset to Factory Defaults

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Reset Factory Defaults**<br>The Reset Factory Defaults page opens. |
| 3 | Select one of the three Reset Factory Defaults options available:<br>**Reset to Factory Defaults AND Erase All Media**<br>Or<br>**Reset to Factory Defaults AND Keep Media**<br>Or<br>**Reset to Factory Defaults AND Re-index Media**. |
| 4 | Click **Apply**. |
| 5 | A warning message displays, click **OK** to continue. |

**- End -**

# NVR Failover, Configuration Backup, Templates and Updates

## Overview

This chapter describes the functionality of the NVR Failover feature, how to create configuration backup files and restore an NVR's settings from the backup file, how to save a configuration template and apply the template to an NVR, and how to apply software updates, patches and update camera handler packs.

## NVR Failover Mode

You can configure an NVR as a Failover NVR using the Enable Failover function.

When in Failover mode, the Failover NVR will monitor other NVR(s) over the network. It monitors all NVR(s) on it's server list until one fails.

When a monitored NVR fails, the Failover Server assumes the role of the failed NVR and NVR monitoring is suspended. The Failover NVR automatically begins to record the IP connected cameras that were recording on the failed NVR. Camera password group information is also transferred to allow the Failover NVR to communicate with the cameras. User account information is not transferred, therefore when prompted to enter a username and password, you must use the Failover NVR username and password.

An NVR that is going to be used as a Failover NVR must be installed and configured in the same way as you would for a normal NVR. You need to configure media folders and storage sets. It is important to note when you are configuring storage for an NVR Failover server, the storage configuration must be able to support recording of any camera configurations set up on any of the NVR's it is monitoring.

Failover monitoring resumes only after the damaged NVR is replaced, and the Failover server is returned to normal operation.

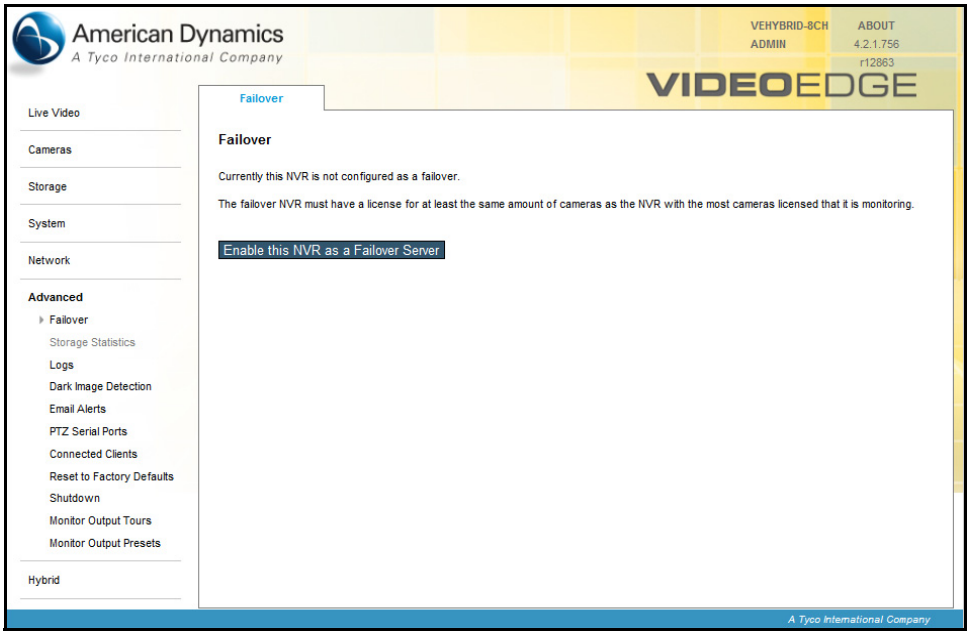
If email alerts are activated for NVR Failover, three emails will be sent during the takeover process. The first email is a notification that failover mode will be activated. The NVR then needs to restart which prompts the second notification, the server has rebooted when the NVR services are being

shut down. The third email is prompted when the server restarts, an activating failover mode notification.

**Note**

The Failover NVR is intended to act as a redundant standby for the NVRs it monitors. The Failover NVR is not intended to manage cameras on its own, because these cameras would no longer be accessible when the Failover NVR takes over for a failed NVR.

**Figure 17-1 Failover Window**



## Configure Failover Mode for an NVR

You must fully configure storage on the Failover NVR that will suit all NVR camera configurations that will be monitored, before configuring and enabling Failover Mode.

### Procedure 17-1
### Configuring Failover Mode for an NVR

| Step | Action |
|---|---|
| 1 | Select **Advanced** from the main menu. |
| 2 | Select **Failover**.<br>The Failover page opens. |
| 3 | Click **Enable this NVR as a Failover Server**. |
| 4 | Click **Add New Server**. |
| 5 | Enter details of the NVR you want the failover NVR to monitor.<br>**a** Enter the Server's IP into the **Server** field.<br>**b** Enter the Server's **Username**.<br>**c** Enter the Server's **Password**.<br>**d** Select the **Enabled** checkbox. |
| 6 | Click **Apply**.<br>The NVR is added to the server monitoring list. |
| 7 | (Optional) Repeat Steps 4 to 6 to add another NVR to monitor. |
| 8 | Select the **Advanced** tab. |
| 9 | Edit the required Failover parameters:<br>**a** **Polling Interval** - Click **Edit**, enter the interval time in seconds and click **Save**. This is how often the failover server checks the live server.<br>**b** **Config Update Interval** - Click **Edit**, enter the interval time in seconds and click **Save**. This is the interval when the failover server checks the live server's configuration and takes a copy of it when it changes.<br>**c** **Heartbeat Timeout** - Click **Edit**, enter the timeout in seconds and click **Save**. This is the timeout of the polling interval.<br>**d** **Retry Count** - Click **Edit**, enter the retry count and click **Save**. This is the number of polling failures until the live server is considered to be inoperable and Failover should begin. |

**- End -**

## Disable Failover Mode

After you have recovered the failed NVR, it will remain in an idle state until the Failover NVR is disabled.

When you disable the Failover NVR, the Failover NVR returns to monitoring the server list.

### Caution

To disable failover mode for an NVR you must disable it from the failover NVR's configuration interface, and not from the interface of any of the monitored NVRs.

### Procedure 17-2
### Disabling Failover Mode

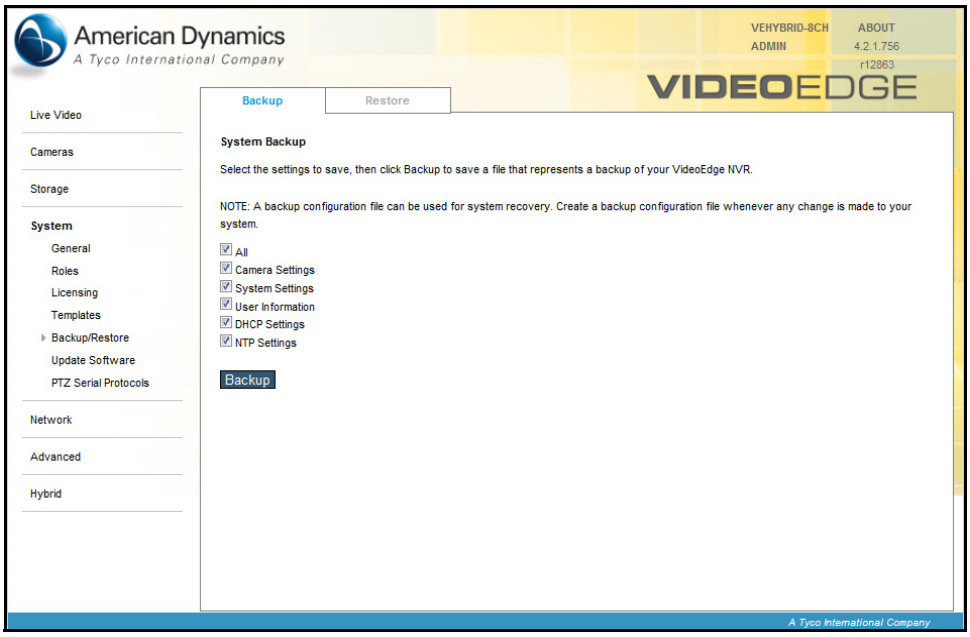
| Step | Action |
|---|---|
| 1 | Select **Advanced** from the main menu. |
| 2 | Select **Failover**.<br>The Failover page opens. |
| 3 | Select the **Disable** tab. |
| 4 | Click **Disable this NVR as a Failover Server**.<br>The Failover server returns to monitoring the server list. |

**- End -**

## Configuration Backup and Restore

With the NVR, you can recover a server's configuration data in the event of a system failure. A system backup file can be stored to a USB or local disk. The backup files can then be imported to the NVR where the saved configuration can be restored.

**Figure 17-2 Backup Window**




## Create a Configuration Backup File

You can create a backup file using the Backup/Restore functionality in the NVR interface. You can choose the type of configuration settings to be stored in the backup file.

**Note**

Operating System settings can not be stored in the configuration backup file. However, the system will also automatically export a text file containing the OS settings which can be used as reference for manually configuring the OS settings.

### Procedure 17-3
### Creating a Configuration Backup File

| Step | Action |
|---|---|

**1** Select **System** from the main menu.

**2** Select **Backup/Restore**.

The Backup page opens.

**3** Select the required checkboxes for the configuration settings that you want saved to the template in the Templates section (Figure 17-2):

- **a** All
- **b** Camera Settings
- **c** System Settings
- **d** User Information
- **e** DHCP Settings
- **f** NTP Settings

4 Click **Backup**.

5 Select **Save As**.

6 Navigate to the folder where you want to save the backup file.

**Note**

To use the backup file during a system recovery procedure you must save the file to an external location, for example, a USB drive.

7 Enter a **File name** for the backup file and click **Save**.

**Note**

A default backup file name is given; this is made up of VideoConfBackup, followed by the NVR name and the date and time the file was created.
Example:
VideoConfBackup-ServerName- yYYYY-mMM-dDD-h00-m00-s00_files.zip
VideoConfBackup-ServerName- y2012-m03-d26-h14-m02-s43_files.zip

This file should be extracted and saved to a safe location not on the NVR. The zip file contains two files, one of the files is the NVR backup information, “VideoConfBackup-xxxxxxxxxxx”. The other is a text file detailing Network and storage mount information, “VideoOSDetails-xxxxxxxx”

**- End -**

## Restore an NVR

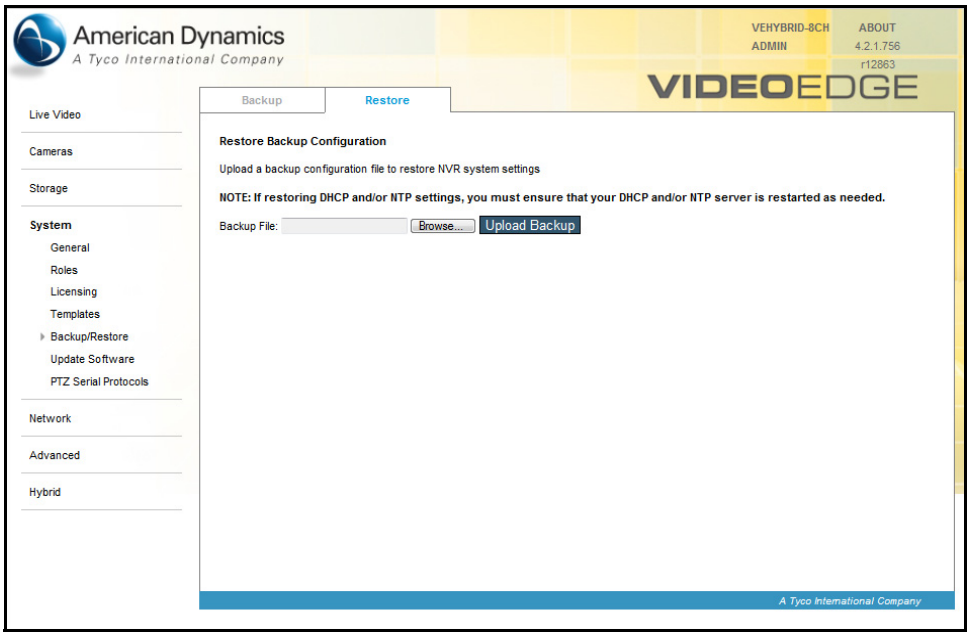
System backup files contain NVR configuration information. The type of information contained in a particular file is dependent on the settings selected when the file was being created. When the backup file is applied, the NVR is restored as per the saved configurations.

**Note**

1 Only a licenced server can be restored.

2 You cannot restore from a previously saved VideoEdge NVR 4.1 backup configuration file.

**Figure 17-3 Restore Window**




## Procedure 17-4
## Restoring an NVR from a Backup File

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Backup/Restore**.<br>The Backup page opens. |
| 3 | Select the **Restore** tab. |
| 4 | Click **Browse**. |
| 5 | Navigate to the backup file you want to use, select the file and click **Open**.<br>A message box opens, asking you if you want to recover any media that is part of storage being restored. |
| 6 | Click **Yes** if you want to recover media, otherwise click **No**. |
| 7 | A recovery progression bar opens and updates as the recovery progresses.<br>If you are recovering media this may take a some time. |
| 8 | A message box opens informing you that the recovery is complete. |
| 9 | Click **OK**. |
| 10 | Configure your network settings using the file “VideoOSDetails-xxxxxxxx”, created as part of your backup file. Use this file as reference to configure: |

- Domain Name
- Domain Name Servers
- Default Gateway
- RTSP Port
- NTP Status
- NTP Servers
- Network Interfaces
- DHCP Configuration

**Note**

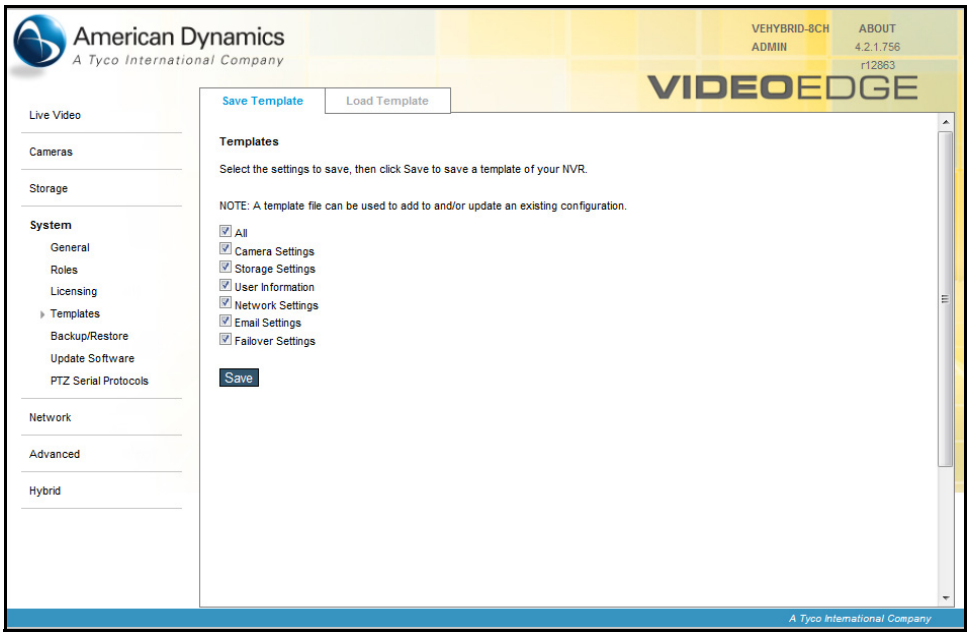
If you are restoring DHCP and/or NTP settings you need to restart your DHCP and/or NTP server.

**- End -**

# Templates

With the NVR, you can save a server's configuration data to a template. You can import the template to another NVR and the configuration settings of the NVR will be configured according to the settings on the imported template. You can store a template file on a USB or local disk.

**Figure 17-4 Template Settings**




## Save a Configuration Template

You can create a configuration template using the Templates functionality in the NVR interface. You can choose the type of configuration settings to be stored in the template. If you want to save camera configuration settings to a template you must ensure that those cameras are connected to the NVR before the template is created.

### Procedure 17-5
### Creating a Configuration Template

| Step | Action |
|---|---|

1 Select **System** from the main menu.

2 Select **Templates**.

The Save Template page opens.

3 Select the required checkboxes for the configuration settings that you want saved to the template:

- **a** All
- **b** Camera Settings
- **c** Storage Settings
- **d** User Information
- **e** Network Settings
- **f** Email Settings
- **g** Failover Settings

4 Click **Save**.

5 Select **Save As**.

6 Navigate to the folder where you want to save the template.

7 Enter a **File name** for the template and click **Save**.

**Note**

A default template file name is given; this is made up of VideoEdgeNVRTemplate, followed by the NVR name and the date and time the template was created.
Example:
VideoEdgeNVRTemplate-ServerName-YYYY-MM-DDT00_00.xml
VideoEdgeNVRTemplate-linux-adnvr-2012-03-26T14_02.xml

**- End -**

## Import a Template File

You can import NVR configuration settings saved as a template. When you are configuring a NVR for the first time, you can load a saved template file, which will configure the NVR with the settings in the file, refer to Procedure 3-14 Configuring the Setup Page on page 28. When applying a template file to an NVR that is already configured, the settings on the NVR will update with the settings saved in the template file. If there are camera configuration settings in the template to be imported, the relevant cameras must be connected to the NVR.

### Procedure 17-6
### Importing a Template File

| Step | Action |
|---|---|

1 Select **System** from the main menu.

2 Select **Templates**.

The Save Template page opens.

3 Select the Load Template tab.

The Load Template page opens.

4 Select the **Import Template** tab.

5 Click **Browse**.

6 Navigate to the template file you want to import.

7 Select the file and click **Open**.

The filepath of the template file appears in the **Template File** field.

8 Click **Apply Template**.

**Note**

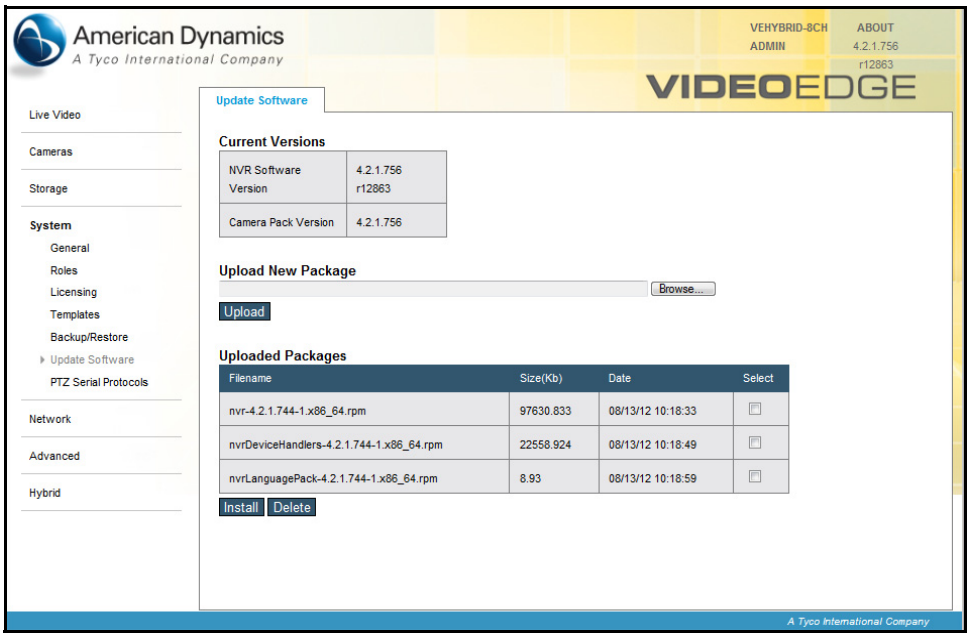
If any errors occur during the template import process, a summary of the errors are displayed.

**- End -**

# Applying Software Updates

You can apply software updates or patches to the NVR using the Update Software page. The current version of the software installed is displayed. To update the software you must upload a new software package and then install the update.

**Figure 17-5 Update Software Page**




## Procedure 17-7
## Update the NVR

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Update Software**.<br>The Update Software page opens (Figure 17-5). |
| 3 | Click **Browse**. |
| 4 | Select the update or patch file and click **Open**.<br>The name and filepath of the patch file appears in the Upload New Package field. |
| 5 | Click **Upload**.<br>The uploaded package is displayed in the Uploaded Packages list. |
| 6 | Select the new package from the list and click **Install.** |

**- End -**

# Updating Camera Handler Packs

Existing camera handlers can be updated or new camera handler packs installed on the NVR, without the need to reload or reboot. Camera handlers can be installed using the Update Software page (Figure 17-5). The current camera pack version is displayed.

**Caution**

Recording and dry contact processing will be stopped for any camera using a handler that is being updated.

## Procedure 17-8
## Updating a Camera Handler Pack

| Step | Action |
|---|---|
| 1 | Select **System** from the main menu. |
| 2 | Select **Update Software**.<br>The Update Software page opens (Figure 17-5). |
| 3 | Click **Browse**. |
| 4 | Select the camera handler pack and click **Open**.<br>The name and filepath of the pack appears in the Upload New Package field. |
| 5 | Click **Upload**.<br>The uploaded package is displayed in the Uploaded Packages list. |
| 6 | Select the new package from the list and click **Install.** |

**- End -**

# Operational Statistics

## Overview

This chapter describes how to view recording statistics, storage statistics and graphs detailing recording performance and disk activity.

## Recording Performance

The Recording Performance page contains a graph displaying the average throughput over time for a selected storage set (Figure 18-1).

**Figure 18-1 Recording Performance Page**

### Procedure 18-1
### Viewing the Recording Performance Statistics

| Step | Action |
|---|---|
| 1 | Select **Advanced** from the main menu. |

2 Select **Storage Statistics**.
The Rec Performance page opens. (Figure 18-1).

3 Select the storage set you want to view the recording performance for from the **Recording Performance** dropdown list.

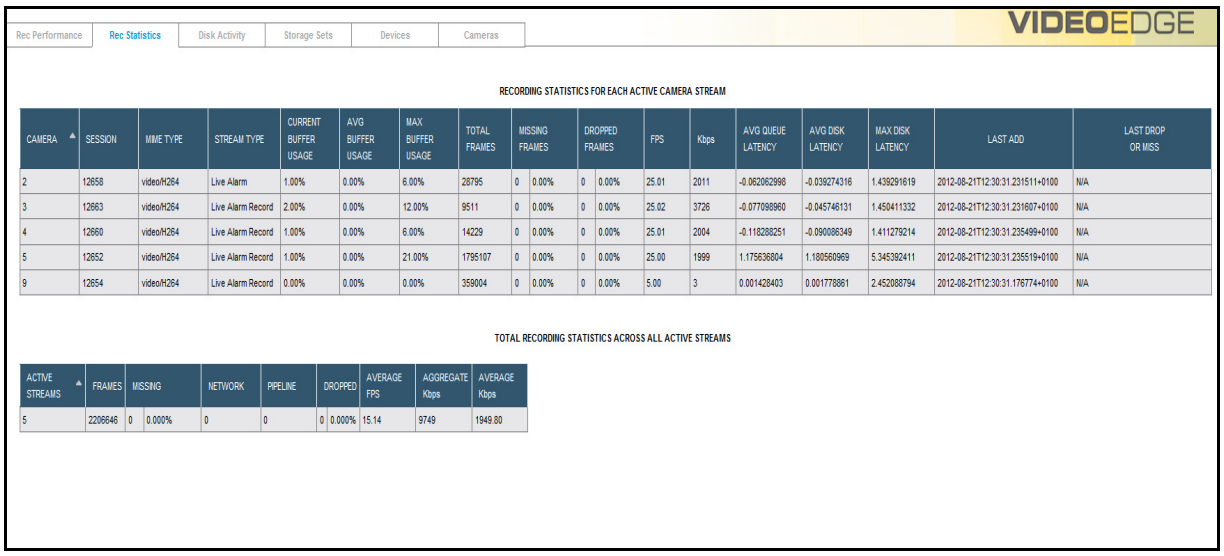
The graph updates displaying details for the selected storage set.

**- End -**

# Recording Statistics

The Recording Statistics page displays recording statistics for each camera configured on the NVR. There is also a Totals summary table displaying recording statistics for the total of all cameras on the NVR. Table 18-1 and Table 18-2 contain details of the recording statistics displayed.

## Figure 18-2 Recording Statistics Page


Rec Performance
Rec Statistics
Disk Activity
Storage Sets
Devices
Cameras
VIDEOEDGE
RECORDING STATISTICS FOR EACH ACTIVE CAMERA STREAM
CAMERA
SESSION
MIME TYPE
STREAM TYPE
CURRENT BUFFER USAGE
AVG BUFFER USAGE
MAX BUFFER USAGE
TOTAL FRAMES
MISSING FRAMES
DROPPED FRAMES
FPS
Kbps
AVG QUEUE LATENCY
AVG DISK LATENCY
MAX DISK LATENCY
LAST ADD
LAST DROP OR MISS
2 12658 video/H264 Live Alarm 1.00% 0.00% 6.00% 28795 0 0.00% 0 0.00% 25.01 2011 -0.062062998 -0.039274316 1.439291619 2012-08-21T12:30:31.231511+0100 N/A
3 12663 video/H264 Live Alarm Record 2.00% 0.00% 12.00% 9511 0 0.00% 0 0.00% 25.02 3726 -0.077098960 -0.045746131 1.450411332 2012-08-21T12:30:31.231607+0100 N/A
4 12660 video/H264 Live Alarm Record 1.00% 0.00% 6.00% 14229 0 0.00% 0 0.00% 25.01 2004 -0.118288251 -0.090086349 1.411279214 2012-08-21T12:30:31.235499+0100 N/A
5 12652 video/H264 Live Alarm Record 1.00% 0.00% 21.00% 1795107 0 0.00% 0 0.00% 25.00 1999 1.175636804 1.180560969 5.345392411 2012-08-21T12:30:31.235519+0100 N/A
9 12654 video/H264 Live Alarm Record 0.00% 0.00% 0.00% 359004 0 0.00% 0 0.00% 5.00 3 0.001428403 0.001778861 2.452088794 2012-08-21T12:30:31.176774+0100 N/A
TOTAL RECORDING STATISTICS ACROSS ALL ACTIVE STREAMS
ACTIVE STREAMS
FRAMES
MISSING
NETWORK
PIPELINE
DROPPED
AVERAGE FPS
AGGREGATE Kbps
AVERAGE Kbps
5 2206646 0 0.000% 0 0 0 0.000% 15.14 9749 1949.80

## Table 18-1 Recording Statistics

| Field | Description |
|---|---|
| Camera | Camera input number. |
| Session | Current active media database session ID associated with stream type for this camera (Note: there will be multiple sessions for the same camera depending on the stream types). |
| MIME Type | Provided details on codec of data recorded in session. |
| Stream Type | Indicates what type of stream recorded for this session, i.e. live, alarm, and or record. |
| Current Buffer Usage | Current percent used of the internal frame buffer (will be 0% if no buffering is occurring, i.e. frames are being written to the disk as they are received). |
| Avg Buffer Usage | Average percent used of the internal frame buffer. |
| Max Buffer Usage | Maximum percent used of the internal frame buffer. |
| Total Frames | Total number of frames recorded in the session. |
| Missing Frames | Total number of missing frames in the session/percent missing. |
| Dropped Frames | Total number of dropped frames in the session (frames inserted into buffer, but the frames were removed before being written due to buffer overflow). |
| FPS | Actual FPS recorded for this camera for this session. |
| Kbps | Calculated Kbps of this camera for this session. |

| Field | Description |
|---|---|
| Avg Queue Latency | Average time between when frame is received and when inserted into queue (seconds). |
| Avg Disk Latency | Average time from queue insertion to disk write (seconds). |
| Max Disk Latency | Maximum time from queue insertion to disk write (seconds). |
| Last Add | Time of last added frame in this session. |
| Last Drop or Miss | Time of last frame dropped/missed if applicable (N/A indicates no frame dropped/missed). |

**Table 18-2 Total Recording Statistics**

| Field | Description |
|---|---|
| Active Streams | Current total number of active streams. |
| Frames | Total number of frames for all cameras. |
| Missing | Total number of missing frames across all cameras. |
| Network | Total number of frames dropped between cameras and NVR (lost over network). |
| Pipeline | Total number of frames dropped from buffer (inserted into buffer but not written). |
| Dropped | Total number of dropped frames across all cameras/percent dropped of total frames. |
| Average FPS | Average FPS of all cameras. |
| Aggregate Kbps | Aggregate Kbps across all cameras. |
| Average Kbps | Average Kbps across all cameras. |

## Procedure 18-2
## Viewing the Recording Statistics

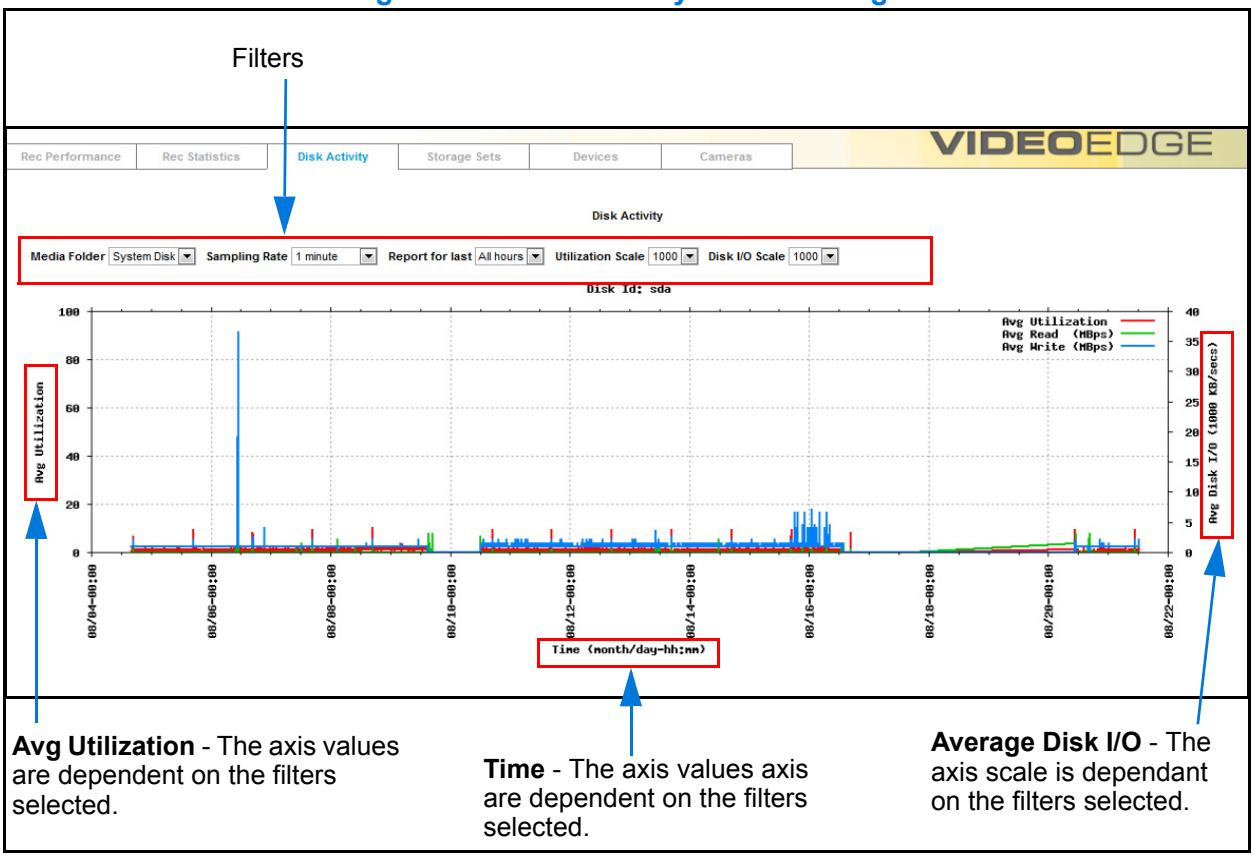
| Step | Action |
|---|---|
| 1 | Select **Advanced** from the main menu. |
| 2 | Select **Storage Statistics**.<br>The Rec Performance page opens. |
| 3 | Select the **Rec Statistics** tab.<br>The Recording Statistics page opens (Figure 18-2). |
| 4 | Details of these statistics are outlined in the **Recording Statistics** table (Table 18-1) or the **Total Recording Statistics** table (Table 18-2). |

**- End -**

# Disk Activity

The Disk Activity page contains a graph outlining the disk activity for a specified media folder over a specified period of time. The graph can be customized by selecting the required filters. There are three values the graph depicts. The Average Utilization (red), the Average Read (green) and the Average Write (blue) over the time period selected.

**Figure 18-3 Disk Activity Statistics Page**




## Procedure 18-3
## Filtering the Disk Activity Graph

| Step | Action |
|---|---|
| 1 | Select **Advanced** from the main menu. |
| 2 | Select **Storage Statistics**.<br>The Rec Performance page opens. |
| 3 | Select the **Disk Activity** tab.<br>The Disk Activity statistics page opens (Figure 18-3). |
| 4 | Select the **Media Folder** you want the graph to display disk activity for from the dropdown. |
| 5 | Select the required **Sampling Rate** from the dropdown. You can select ranges between 1 minute and 120 minutes. |
| 6 | Choose the number of hours you want the graph to display disk activity for. Select this from the **Report for last** dropdown. |

7 Select the **Utilization Scale** from the dropdown.

8 Select the **Disk I/O Scale** from the dropdown.

The graph adjusts to display the disk activity as per the filters selected.

**- End -**

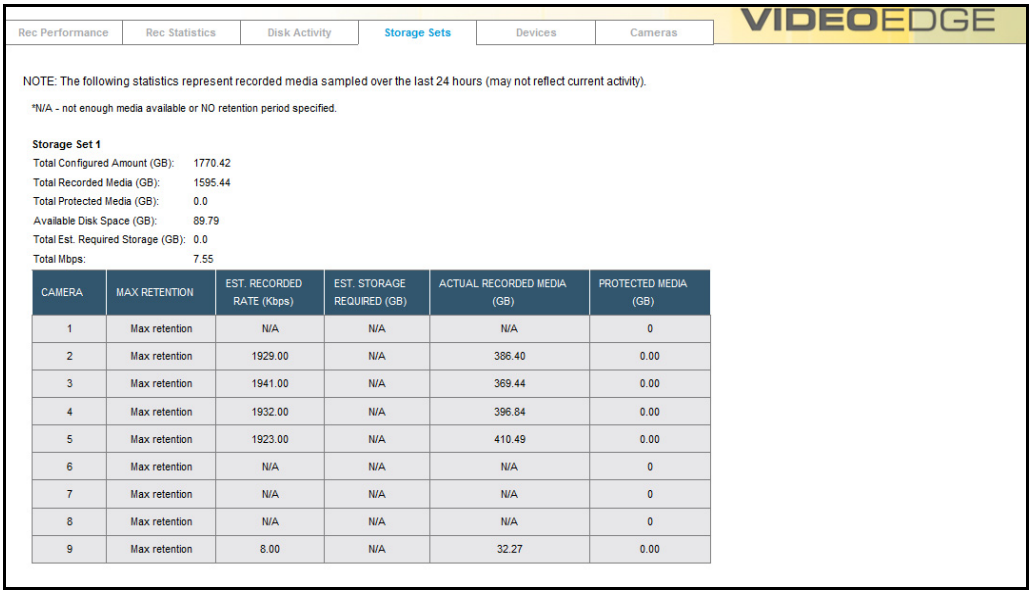
# Storage Statistics

The NVR holds and displays storage statistics for storage sets, storage devices and cameras that are being used in the NVR storage configuration.

## Storage Set Statistics

The Storage Set page contains statistics for the total amount of storage available in each storage set. This is the combined storage available from all storage devices assigned to the storage set and does not contain information on individual device statistics. The storage set section also contains statistics for each camera assigned to each storage set. Further information on the data provided can be found in Table 18-3.

**Figure 18-4 Storage Statistics Page**


Rec Performance
Rec Statistics
Disk Activity
Storage Sets
Devices
Cameras
VIDEOEDGE
NOTE: The following statistics represent recorded media sampled over the last 24 hours (may not reflect current activity).
*N/A - not enough media available or NO retention period specified.
Storage Set 1
Total Configured Amount (GB): 1770.42
Total Recorded Media (GB): 1595.44
Total Protected Media (GB): 0.0
Available Disk Space (GB): 89.79
Total Est. Required Storage (GB): 0.0
Total Mbps: 7.55
CAMERA | MAX RETENTION | EST. RECORDED RATE (Kbps) | EST. STORAGE REQUIRED (GB) | ACTUAL RECORDED MEDIA (GB) | PROTECTED MEDIA (GB)
1 | Max retention | N/A | N/A | N/A | 0
2 | Max retention | 1929.00 | N/A | 386.40 | 0.00
3 | Max retention | 1941.00 | N/A | 369.44 | 0.00
4 | Max retention | 1932.00 | N/A | 396.84 | 0.00
5 | Max retention | 1923.00 | N/A | 410.49 | 0.00
6 | Max retention | N/A | N/A | N/A | 0
7 | Max retention | N/A | N/A | N/A | 0
8 | Max retention | N/A | N/A | N/A | 0
9 | Max retention | 8.00 | N/A | 32.27 | 0.00

### Table 18-3 Storage Set Statistics

| Field | | Description |
|---|---|---|
| Storage | Total Configured Amount (GB) | Total configured amount of storage that will be used in this storage set. |
| | Total Recorded Media (GB) | Current total amount of recorded media in this storage set. |
| | Total Protected Media (GB) | Current total amount of protected media in this storage set. |
| | Available Disk Space (GB) | Total available disk space in this storage set. |
| | Total Est. Required Storage (GB) | If a retention period is defined on any camera this will show the total required storage needed to support those retention values, otherwise 0.0. |
| | Total Mbps | Current calculated Mbps for this storage set. |
| Camera | Camera | Input number. |
| | Max Retention | Current configured retention period. |
| | Est. Record Rate (Kbps) | Current Kbps over last 24 hour period (if less than 24 hours will display N/A) |
| | Est. Storage Required (GB) | If a retention period is specified, this will indicate the required storage needed to support that retention period. |
| | Actual Recorded Media (GB) | Actual amount of recorded media for this camera in this storage set. |
| | Protected Media (GB) | Amount of current protected media for this camera in this storage set. |

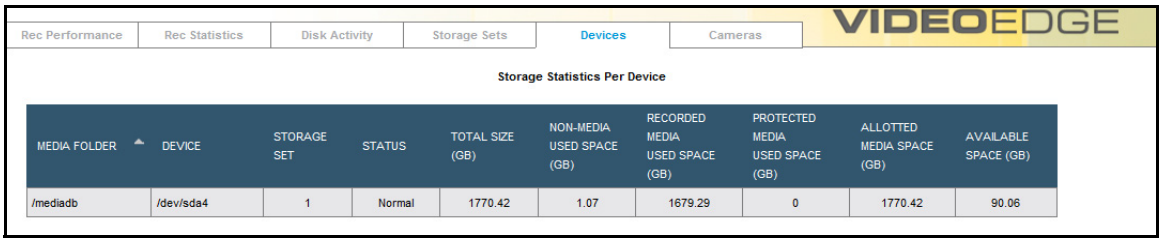
**Note**

If a camera has stored media in a storage set but has now been assigned to another or has been deleted, the camera number will be displayed followed by **. This indicates the camera is not currently configured in this storage set. The Max Retention, Recorded Rate (Kbps) and Est. Storage Required (GB) will display as **Unknown**. The Actual Recorded Media (GB) and Protected Media (GB) will display their values.

## Storage Device Statistics

The Devices page contains storage statistics per individual storage device. For information on the data provided, see Table 18-4.

### Figure 18-5 Storage Statistics per Device



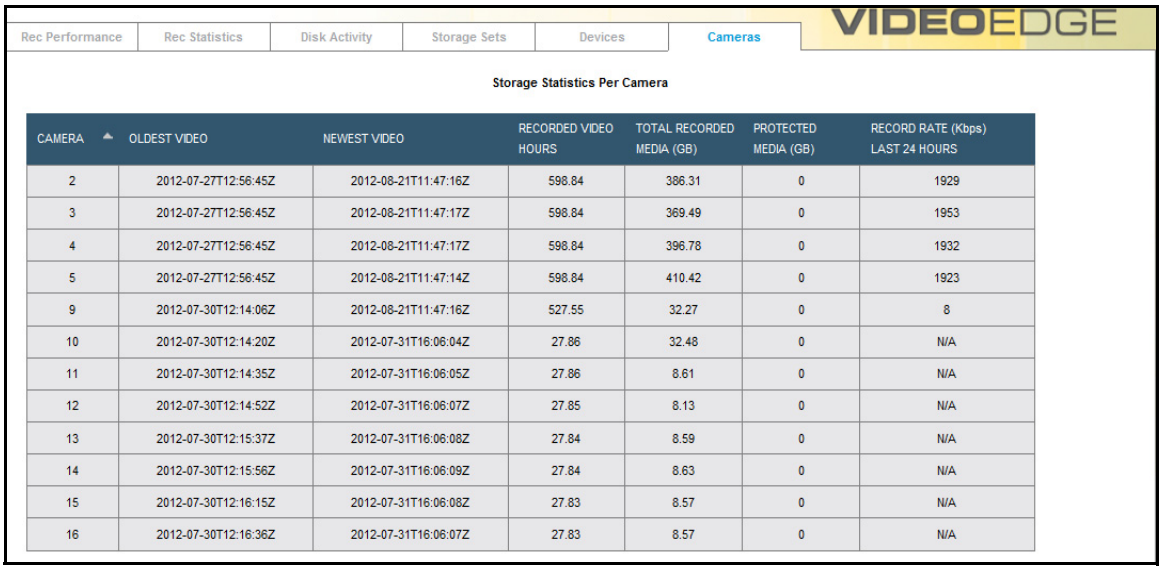

### Table 18-4 Storage Device Statistics

| Field | Description |
|---|---|
| Media Folder | Name of the media folder used by storage. |
| Device | Associated device on which this media folder is located. |
| Storage Set | Storage set this media folder is assigned to. |
| Status | Current Status of this folder (Normal, Degraded and so on). |
| Total Size (GB) | Total size of this device. |
| Non-Media Used Space (GB) | Total amount of space used by non NVR media files (if any) on this device. |
| Recorded Media Used Space (GB) | Total amount of space used for NVR recorded media at this time. |
| Protected Media Used Space (GB) | Total amount of space used for protected media on this device. |
| Allotted Media Space (GB) | Configured amount to use for storage on this device. |
| Available Space (GB) | Current total available unused space on this device. |

## Storage Statistics per Camera

The Cameras page details the storage statistics for each camera. These are outlined in Table 18-5.

## Figure 18-6 Storage Statistics per Camera




## Table 18-5 Camera Storage Statistics

| Field | Description |
|---|---|
| Camera | Input number. |
| Oldest Video | Time of oldest video for this camera across all storage sets. |
| Newest Video | Time of newest video for this camera across all storage sets. |
| Recorded Video Hours | Total number of recorded video hours for this camera across all storage sets. |
| Total Recorded Media (GB) | Total amount of recorded media for this camera across all storage sets. |
| Protected Media (GB) | Total amount of protected media for this camera across all storage sets. |
| Record Rate (Kbps) Last 24 Hours | Record rate for this camera over the last 24 hours (N/A -if less than 24 hours of data). |

## Procedure 18-4
## Viewing Storage Statistics

| Step | Action |
|---|---|

**1** Select **Advanced** from the main menu.

**2** To view storage set statistics select **Storage Sets** page.

Or

To view device statistics select **Device** page.

Or

To view camera statistics select **Cameras** page.

The required statistics are displayed. For further information refer to Table 18-3, Table 18-4 or Table 18-5.

**- End -**

# Logs

## Overview

This chapter describes the features of the Logs submenu and the Connected Clients sub menu.

The NVR tracks important types of system events. You can view logs of the following:

- Administrative changes
- Camera alerts
- Changes to cameras
- System events (used by American Dynamics technical support)

The Logs page provides access to the NVRs log settings, this allows you to retrieve logs, edit the FTP Log Management settings, filter searches for Events Logs, view Camera Connection Errors, Camera Logs and an Audit Trail.

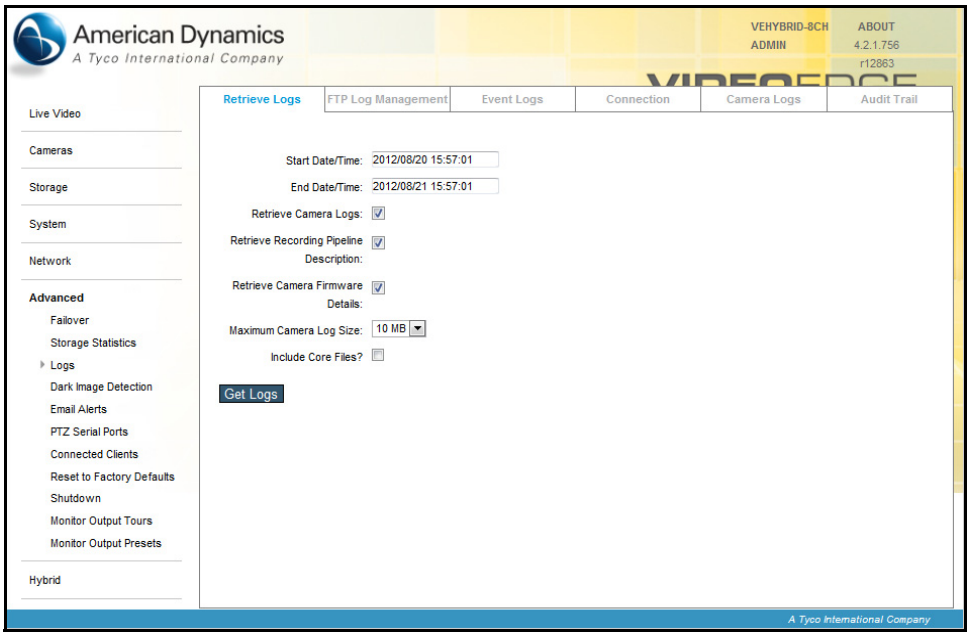
Using the Connected Clients page you can view a summary of the victor clients which are currently streaming video from the NVR.

## Retrieving Logs

The Retrieve Logs page provides you the ability to customise the search criteria for retrieving log files. The editable criteria includes a date and time range, selection options for retrieving camera logs, recording pipeline descriptions, camera firmware details and core files. A dropdown also provides selectable maximum camera log sizes of; 1Mb, 5Mb, 10Mb, 25Mb and 50Mb.

The retrieved log file is in zipped format, it can either be opened as a temporary folder or saved local using the Windows file download window or other OS equivalent.

### Figure 19-1 Retrieve Logs Page




## Procedure 19-1
## Retrieving Logs

| Step | Action |
|---|---|

**1** Select **Advanced**.

**2** Select **Logs**.

The Retrieve Logs page opens.

**3** Type the Start Date/Time in the **Start Date/Time** text box.

**Note**

Enter in the following format; Year/Month/Date Hours:Minutes:Seconds. For example for 1pm on 21st January 2012 would be **2012/01/21 13:00:00**.

Or

Select the Start Date/Time field and a calendar opens. You can use the calendar to select the date and use the sliders to adjust the time.

**4** Type the End Date/Time in the **End Date/Time** text box in the same format described in step 3.

**5** Select/deselect the **Retrieve Camera Logs** check box as required.

**6** Select/deselect the **Retrieve Recording Pipeline Description** checkbox as required.

**7** Select/deselect the **Retrieve Camera Firmware details** checkbox as required.

**8** Using the **Maximum Camera Log Size** dropdown select the maximum camera log size.

**9** Select/deselect the **Include Core Files** checkbox as required.

**10** Click **Get Logs**.

**11** When the File Download window displays Click **Open** or **Save**.

The Logs folder is now ready to be viewed.

**- End -**

# FTP Log Management

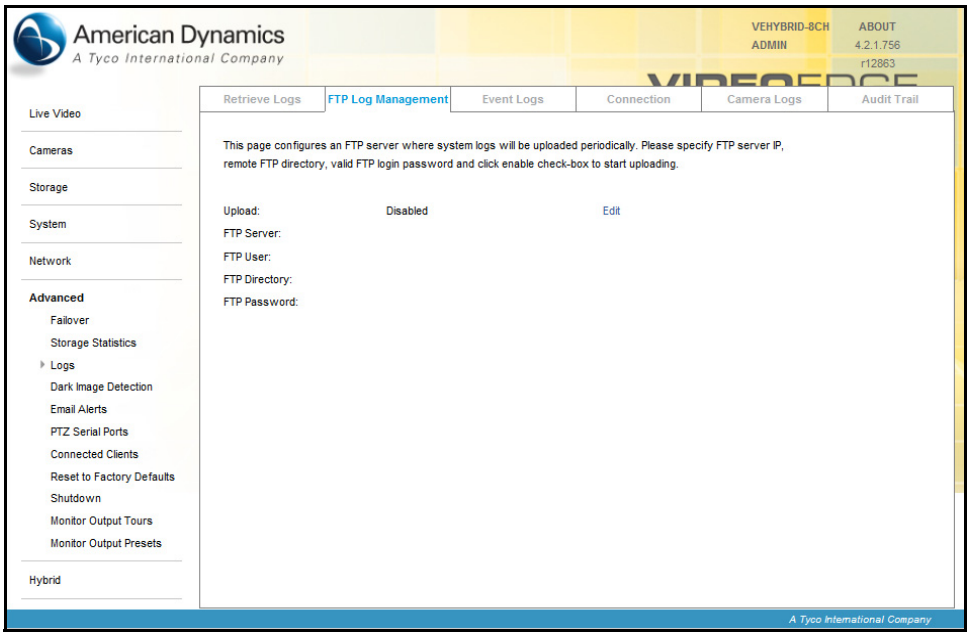
The FTP Log Management page allows you to configure FTP server settings where system logs will be uploaded periodically. The Event Log is rotated (all entries are cleared) when it is full. To preserve the Events Log this function should be configured and enabled.

**Note**

Only syslog files are uploaded when using this feature.

The FTP Log Management page allows you to input the FTP server IP Address, FTP Username, remote FTP Directory and FTP Password. A valid Default Gateway must be assigned in the General Network Settings to use this feature.

**Figure 19-2 FTP Log Management Page**




## Procedure 19-2
## Editing Settings for the Log FTP Server

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Logs**. |

3 Select the **FTP Log Management** tab.

The FTP Log Management page opens.

4 Select **Edit**.

5 Select the **Enabled** option button to enable Event Log upload to the FTP Server.

6 Enter the IP Address in the **FTP Server** field.

7 Enter the username in the **FTP User** field.

8 Enter the directory in the **FTP Directory** field.

9 Enter the password in the **FTP Password** field.

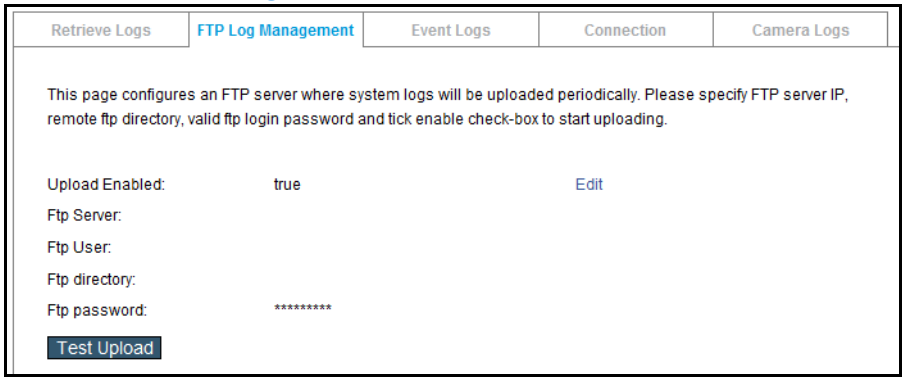
10 Enter the password again in the **Confirm Password** field.

11 Click **Save**.

**Note**

When FTP Log upload is enabled, a **Test Upload** button displays. This button can be used to verify the FTP server settings. A successful upload test will create a test file on the specified location of the FTP Server.

**Figure 19-3 Test Upload Button**




**- End -**

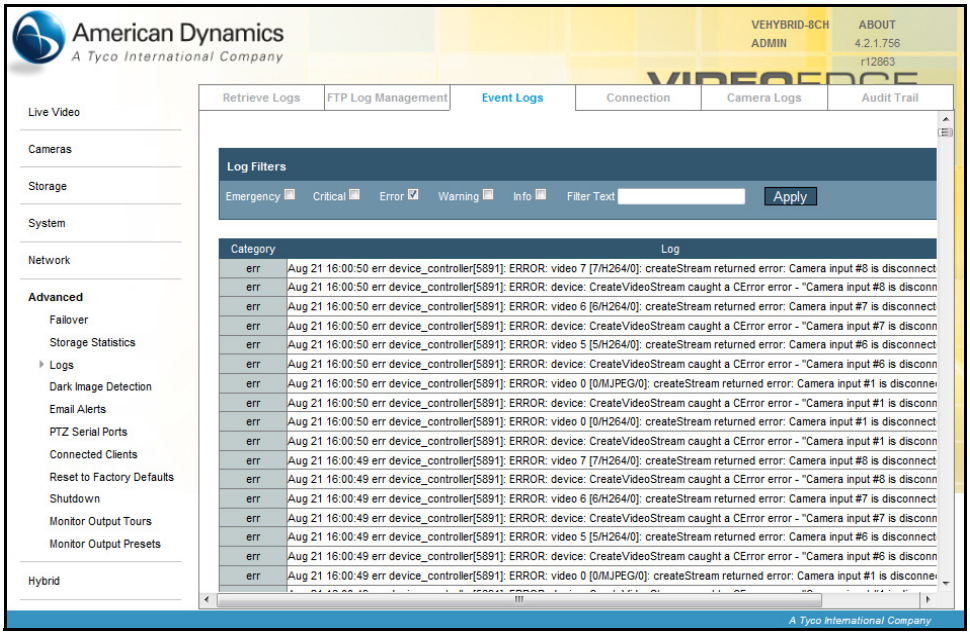
# Event Logs

The Event Logs page is used primarily by American Dynamics technical support for troubleshooting. The Event Log shows informational and error-related events that have occurred on the NVR system.

When the Event Log is full, the file is rotated (all entries are cleared) and a new Event Log is started.

The Event Log page provides a filter feature. You can filter by the following criteria; Emergency, Critical, Error, Warning, Info and Filter Text.

**Figure 19-4 Event Logs Page**




## Procedure 19-3
## Viewing Event Logs

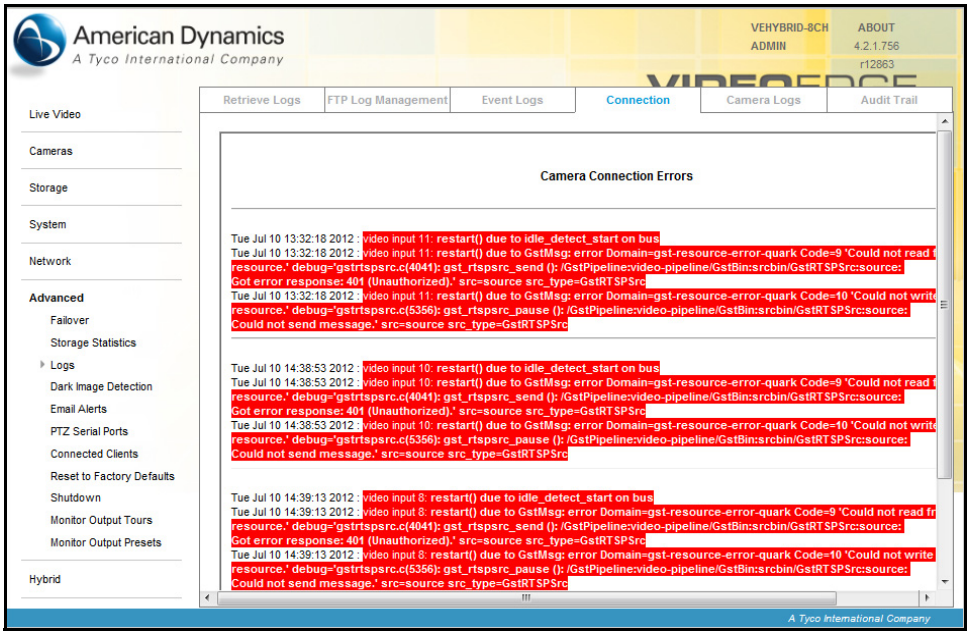
| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Logs**. |
| 3 | Select the **Event Logs** tab.<br>The Event Logs page opens. |
| 4 | To include emergency event logs, select the **Emergency** checkbox. |
| 5 | To include critical event logs, select the **Critical** checkbox. |
| 6 | To include error event logs, select the **Error** checkbox. |
| 7 | To include warning event logs, select the **Warning** checkbox. |
| 8 | To include info event logs, select the **Info** checkbox. |
| 9 | To include specific filter text, enter the desired filter text in the **Filter text** textbox. |
| 10 | Click **Apply**. |

**- End -**

# Camera Connection Errors

The Connection page displays the Camera Connection Errors that have occurred.

**Figure 19-5 Connection Page**


American Dynamics
A Tyco International Company
VEHYBRID-8CH
ADMIN
ABOUT
4.2.1.756
r12863
Retrieve Logs
FTP Log Management
Event Logs
Connection
Camera Logs
Audit Trail
Live Video
Cameras
Storage
System
Network
Advanced
Failover
Storage Statistics
Logs
Dark Image Detection
Email Alerts
PTZ Serial Ports
Connected Clients
Reset to Factory Defaults
Shutdown
Monitor Output Tours
Monitor Output Presets
Hybrid
Camera Connection Errors
Tue Jul 10 13:32:18 2012 : video input 11: restart() due to idle_detect_start on bus
Tue Jul 10 13:32:18 2012 : video input 11: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=9 'Could not read
resource.' debug='gstrtspsrc.c(4041): gst_rtspsrc_send (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Got error response: 401 (Unauthorized).' src=source src_type=GstRTSPSrc
Tue Jul 10 13:32:18 2012 : video input 11: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=10 'Could not write
resource.' debug='gstrtspsrc.c(5356): gst_rtspsrc_pause (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Could not send message.' src=source src_type=GstRTSPSrc
Tue Jul 10 14:38:53 2012 : video input 10: restart() due to idle_detect_start on bus
Tue Jul 10 14:38:53 2012 : video input 10: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=9 'Could not read
resource.' debug='gstrtspsrc.c(4041): gst_rtspsrc_send (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Got error response: 401 (Unauthorized).' src=source src_type=GstRTSPSrc
Tue Jul 10 14:38:53 2012 : video input 10: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=10 'Could not write
resource.' debug='gstrtspsrc.c(5356): gst_rtspsrc_pause (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Could not send message.' src=source src_type=GstRTSPSrc
Tue Jul 10 14:39:13 2012 : video input 8: restart() due to idle_detect_start on bus
Tue Jul 10 14:39:13 2012 : video input 8: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=9 'Could not read fr
resource.' debug='gstrtspsrc.c(4041): gst_rtspsrc_send (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Got error response: 401 (Unauthorized).' src=source src_type=GstRTSPSrc
Tue Jul 10 14:39:13 2012 : video input 8: restart() due to GstMsg: error Domain=gst-resource-error-quark Code=10 'Could not write
resource.' debug='gstrtspsrc.c(5356): gst_rtspsrc_pause (): /GstPipeline:video-pipeline/GstBin:srcbin/GstRTSPSrc:source:
Could not send message.' src=source src_type=GstRTSPSrc
A Tyco International Company

## Procedure 19-4
## Viewing Camera Connection Errors

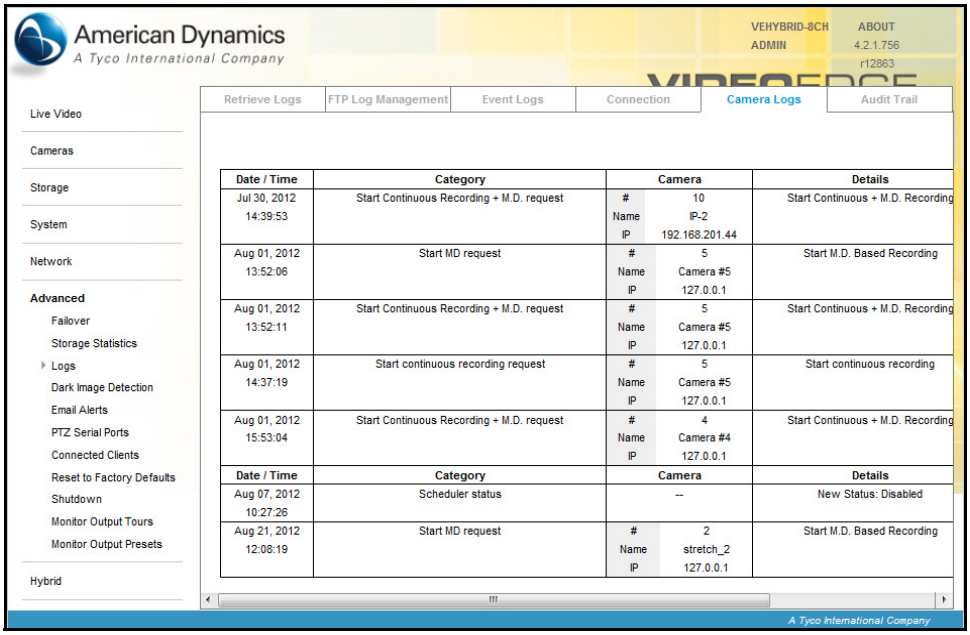
| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Logs**. |
| 3 | Select the **Connection** tab.<br>The Connection page opens. |

**- End -**

# Camera Logs

The Camera Log page provides information on camera reboots, changes to camera recording status, and the use of the Pan-Tilt-Zoom (PTZ) and other controls.

## Figure 19-6 Camera Logs Page




## Table 19-1 Camera Logs Definitions

| Column | Description |
|---|---|
| Date/Time | Displays the Date and Time that the camera reported a change. |
| Category | Lists the type of action or change that occurred. |
| Camera | Lists the camera number, name and IP Address. |
| Details | Displays the details of the action or change that occurred. |
| Operator | Displays the name of the user who initiated the action. |
| Client Machine | Lists the IP Address of the client machine from which the user-initiated action originated. |

## Procedure 19-5
## Viewing the Camera Logs

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Logs**. |
| 3 | Select the **Camera Logs** tab.<br>The Camera Logs page opens. |

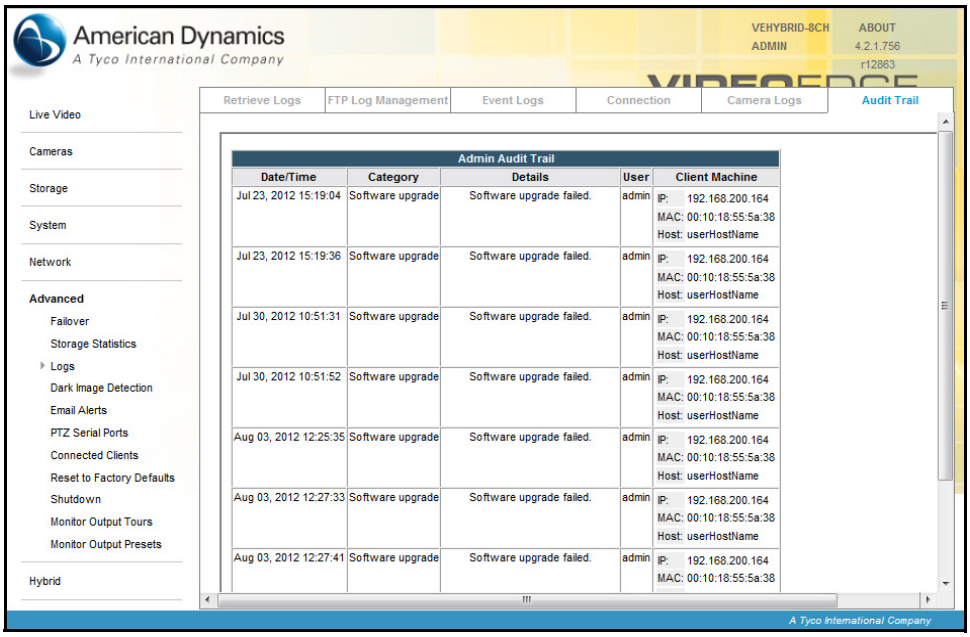
**- End -**

# Audit Trail

The Audit Trail page displays a log of system changes which have been made by a privileged user. The system changes which are logged in the Audit Trail are:

1. System Date and Time
2. Software upgrade
3. FTP Log Management settings
4. User Login Passwords
5. Network Settings

**Figure 19-7 Audit Trail Page**


American Dynamics
A Tyco International Company
VEHYBRID-8CH
ADMIN
ABOUT
4.2.1.756
r12863
Retrieve Logs
FTP Log Management
Event Logs
Connection
Camera Logs
Audit Trail
Live Video
Cameras
Storage
System
Network
Advanced
Failover
Storage Statistics
Logs
Dark Image Detection
Email Alerts
PTZ Serial Ports
Connected Clients
Reset to Factory Defaults
Shutdown
Monitor Output Tours
Monitor Output Presets
Hybrid
Admin Audit Trail
Date/Time
Category
Details
User
Client Machine
Jul 23, 2012 15:19:04 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Jul 23, 2012 15:19:36 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Jul 30, 2012 10:51:31 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Jul 30, 2012 10:51:52 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Aug 03, 2012 12:25:35 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Aug 03, 2012 12:27:33 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38 Host: userHostName
Aug 03, 2012 12:27:41 Software upgrade Software upgrade failed. admin IP: 192.168.200.164 MAC: 00:10:18:55:5a:38
A Tyco International Company

## Procedure 19-6
## Viewing the Audit Trail

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Logs**. |
| 3 | Select the **Audit Trail** tab.<br>The Audit Trail page opens. |

**- End -**

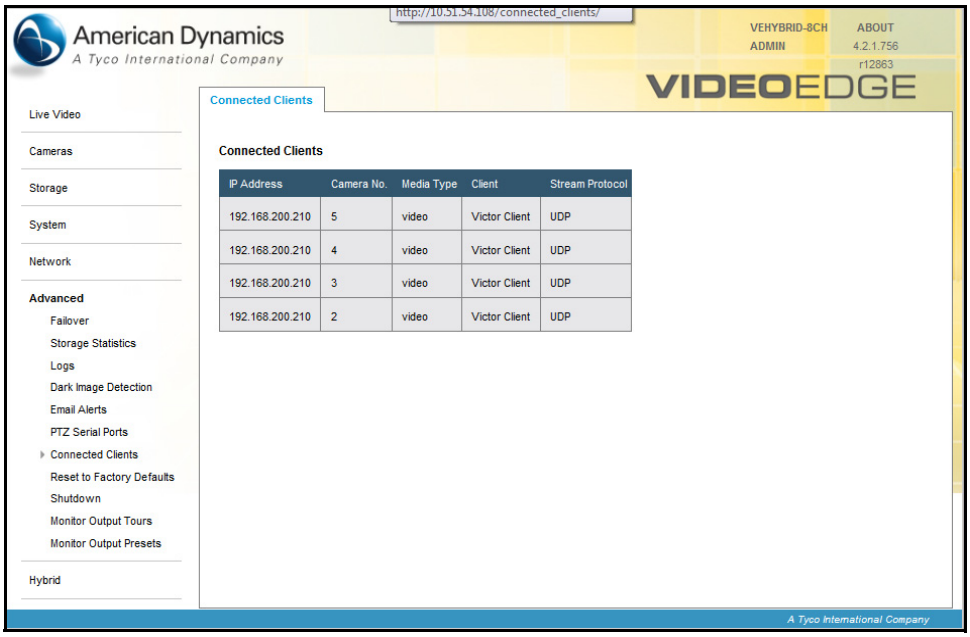
# Viewing Connected Clients

You can view the clients currently connected to the NVR using the Connected Clients sub menu. The NVR will only register a client as connected if it is actively receiving a video/audio stream from the NVR.

The Connected Client page displays information relating to the clients currently connected to the NVR and their activity. The following information is displayed when a client is connected to the NVR:

- The IP Address of the device which is streaming audio and video from the NVR via victor unified client.
- The Camera Number for each camera being streamed from the NVR for each client connected to the NVR.
- The Media Type being streamed; either audio or video or both.
- The Client type, for example victor unified client or QuickTime.
- The Streaming Protocol being used.

**Figure 19-8 Connected Clients Page**




## Procedure 19-7
## Viewing Connected Clients

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Connected Clients**.<br>The Connected Clients page opens. |

**- End -**

# Email Alerts

## Overview

The Email Alerts page consists of the Email Alerts page and the Alert Logs page. Email Alerts can be setup in the NVR to send notifications to selected email addresses regarding several different categories, see Table 20-1.

The Alert Logs page is used to display all of the email alerts that have been transmitted.

**Table 20-1 Alert Categories**

| Alert Category | Description |
|---|---|
| System Alerts | All general system alerts not included in the other categories. |
| Storage Alerts | Transmitted when storage is not healthy. |
| Motion Detection Alerts | Generated by motion detection. Does not include image attachments. |
| Analytics Alerts | Generated by Video Intelligence Alerts. |
| Camera Malfunction | Sent when a camera refuses to respond. |
| Reboot Notification | Sent when the system is rebooted. |
| Camera(s) Not Recording | Generated when recording does not occur on one or more cameras. |
| No Storage Active on Unit | Generated when no storage can be activated. |
| Failed to Read Storage Config | Sent when storage configuration errors occur. |
| Failover Event | Sent when a failover is detected. The IP address of the NVR which has failed will be included. |

**Note**

In order to use the email notification feature, you must have the IP address of an SMTP switch or a mail server; ask your IT administrator for details.

## Advance Preparation

Prior to configuring email alerts you must ensure that you have a valid Domain Name and Default Gateway configured in the network settings of the NVR network.

### Procedure 20-1
### Advance Preparation for Email Alerts

| Step | Action |
|---|---|
| 1 | Select **Network**. |
| 2 | Select **General**.<br>The Network General page opens. |
| 3 | To edit the **Domain Name** select the current value. Update the Domain Name as required.<br>The field background changes to yellow indicating a change has been made. |
| 4 | To edit the **Default Gateway** select the current value. Update the Default Gateway as required.<br>The field background changes to yellow indicating a change has been made. |
| 5 | Click **Save**.<br>A validation message displays. |

**Note**

The NVR will send notifications to email addresses sharing its own domain. Additionally, it can send notifications to email addresses in other domains provided those domains' SMTP servers have allowed incoming emails from the NVR's domain. Owners of email addresses in other domains should contact their email administrator to ensure they will be able to receive alert notifications from the NVR's domain. The delivery of email notifications sent to email addresses provided by Internet Service Providers (ISPs, such as, Yahoo or Gmail) cannot be guaranteed because those ISPs have their own restrictions that may interfere.

**- End -**

# Setting Up Email Alerts

To set up email notifications you are required to build the recipient list and enable the notifications each address on the recipient list is to receive.

## SMTP Server IP Address

To allow the Email Alerts functionality with the NVR you must enter the SMTP Server IP address.

### Procedure 20-2
### Entering the SMTP Server IP Address

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |

2 Select **Email Alerts**.

The Email Alerts page opens.

3 Click **EDIT** next to the SMTP Server IP field.

4 Enter the **SMTP Server IP address** in the field.

5 Click **Save**.

**- End -**

## Building the Recipient List

The recipient list is made up of email addresses which will receive email alerts. The alerts that each address will receive is defined by the alert category associated with that address and whether or not that category has been enabled.

### Procedure 20-3
### Building the Recipient List

| Step | Action |
|---|---|

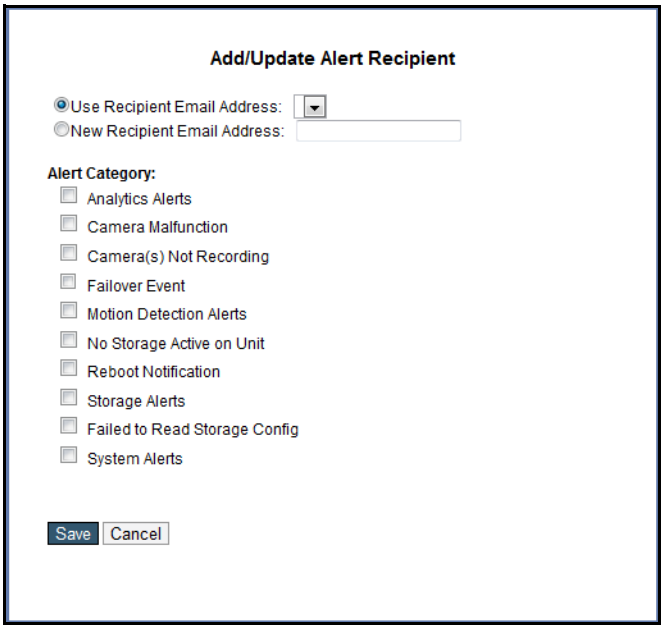
1 Select **Advanced**.

2 Select **Email Alerts**.

The Email Alerts page opens.

3 Click **Add/Update Alert Recipient**.

The Add/Update Alert Recipient pop up displays.




4 Select the **New Recipient Email Address** option button.

5 Enter the recipient's email address in the field.

Or

If the user is already receiving notifications, you can choose the user's email address from the **Use Recipient Email address** dropdown menu.

6 Select the **Alert Categories** using the checkboxes.

7 Click **Save**.

8 Verify that the email address has been added to the recipient list for each alert category. You can check by viewing recipients for each alert category listed in the table on the Email Alerts page refer to Figure 20-1 Alert Category Recipients on page 212.

**Figure 20-1 Alert Category Recipients**

9 To send a test email to a recipient list, select the alert you wish to test an click **Test**.

10 Once you have the email recipients configured, you need to enable alerts. Refer to Enabling and Disabling Email Alerts on page 212.

**- End -**

## Enabling and Disabling Email Alerts

Once recipient addresses have been entered and alert categories assigned you can configure which email alerts should be enabled for each recipient.

### Procedure 20-4
### Enabling and Disabling Email Alerts

| Step | Action |
|---|---|

1 Select **Advanced**.

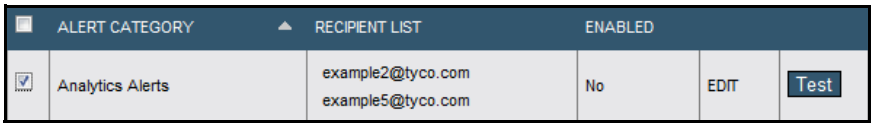
2 Select **Email Alerts**.

The Email Alerts page opens.

3 Select the checkbox for each alert you wish to enable from the **Alert Category** list.

4 Click **Enable Alert(s)**.

**Figure 20-2 Enabling and Disabling Email Notifications**




5 After enabling email alerts, an email is sent to the selected recipients when the appropriate alert is triggered.

**- End -**

## Disabling Email Alerts for a Camera

You can disable Email Alerts for a specific camera. This allows you to suppress email alerts from cameras which are known to be malfunctioning.

### Caution

This procedure will disable the cameras ability to stream live video.

Attempting to modify some of the parameters of the camera such as Password Group or PTZ will not be possible when the camera is disabled.

### Procedure 20-5
### Disabling Email Alerts for a Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras**. |
| 2 | Select **List**.<br>The Camera List page opens. |
| 3 | Click **Setup** in the camera record of the camera you wish to disable email alerts.<br>The Function & Streams page opens. |
| 4 | Select the **General** tab.<br>The General page opens. |
| 5 | Click the Camera Streaming **Disable** option button. |
| 6 | Click **Apply**.<br>In the camera record on the Camera List page the IP address indicates **DISABLED**. |

**- End -**

### Procedure 20-6
### Re-enabling Email Alerts for a Camera

| Step | Action |
|---|---|
| 1 | Select **Cameras**. |
| 2 | Select **List**.<br>The Camera List page opens. |
| 3 | Click **Setup** in the camera record of the camera you wish to re-enable email alerts.<br>The Function & Streams page opens. |
| 4 | Select the **General** tab.<br>The General page opens. |
| 5 | Click the Camera Streaming **Enable** option button. |
| 6 | Click **Apply**.<br>In the camera record on the Camera List page the IP address no longer indicates **DISABLED**. |

**- End -**

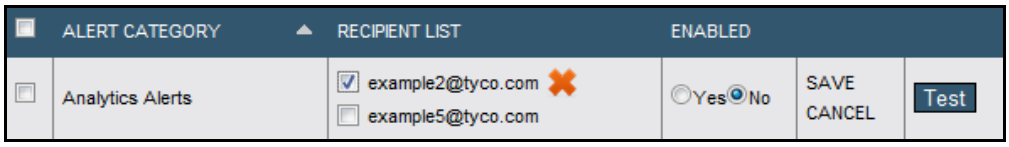
## Removing an Address from the Recipient List

You can remove recipient addresses from each alert category.

### Procedure 20-7
### Remove an Address from the Recipient List

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 1 | Select **Email Alerts**.<br>The Email Alerts page opens. |
| 2 | Scroll to the **Alert Category** you wish to remove a recipients address from. |
| 3 | Select **Edit**. |
| 4 | Select the checkbox next to the address you wish to remove. |

**Figure 20-3 Deleting Email Addresses from a Recipient List**



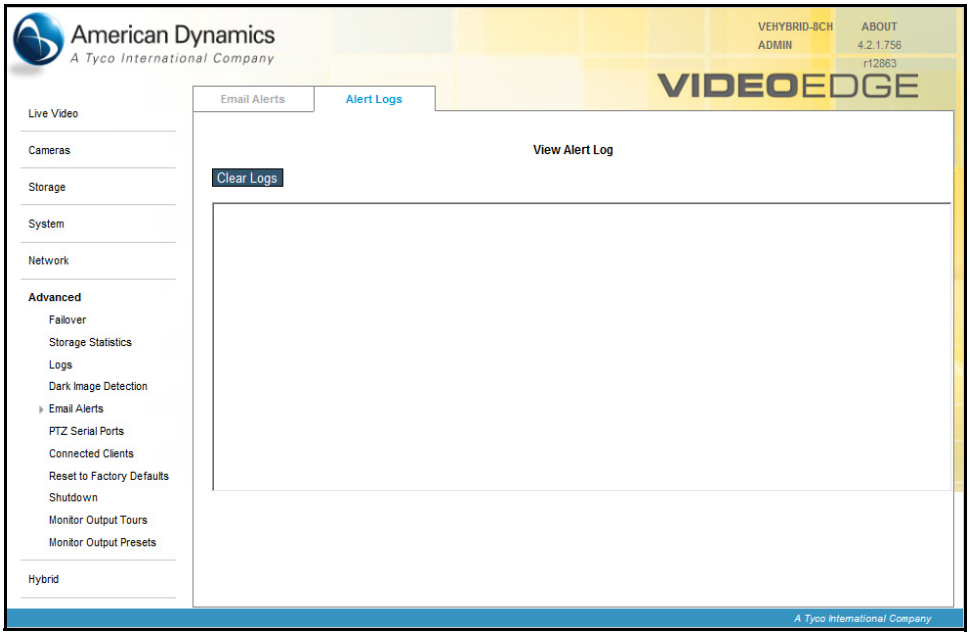

**5** Select **Save**.
The page refreshes and the address is removed from the recipient list.

**- End -**

## Alert Logs

The Alert Logs page displays a list of email alerts which have been sent by the NVR. Each entry includes the recipient email address, alert type and information sent with the time and date the alert occurred.

**Figure 20-4 Alert Logs Page**




### Procedure 20-8
### Displaying the Email Alerts Log

| Step | Action |
|---|---|

**1** Select **Advanced**.

**2** Select **Email Alerts**.

**3** Select the **Alert Logs** tab.

The Alert Logs page opens.

**- End -**

## Clearing the Alert Logs Page

All email alerts can be cleared from the Alert Logs page.

### Procedure 20-9
### Clearing the Alert Logs Page

| Step | Action |
|---|---|
| **1** | Select **Advanced**. |
| **2** | Select **Email Alerts**. |
| **3** | Select the **Alert Logs** tab.<br>The Alert Logs page opens. |
| **4** | Click **Clear Logs**. |

**- End -**

# Dark Image Detection

## Overview

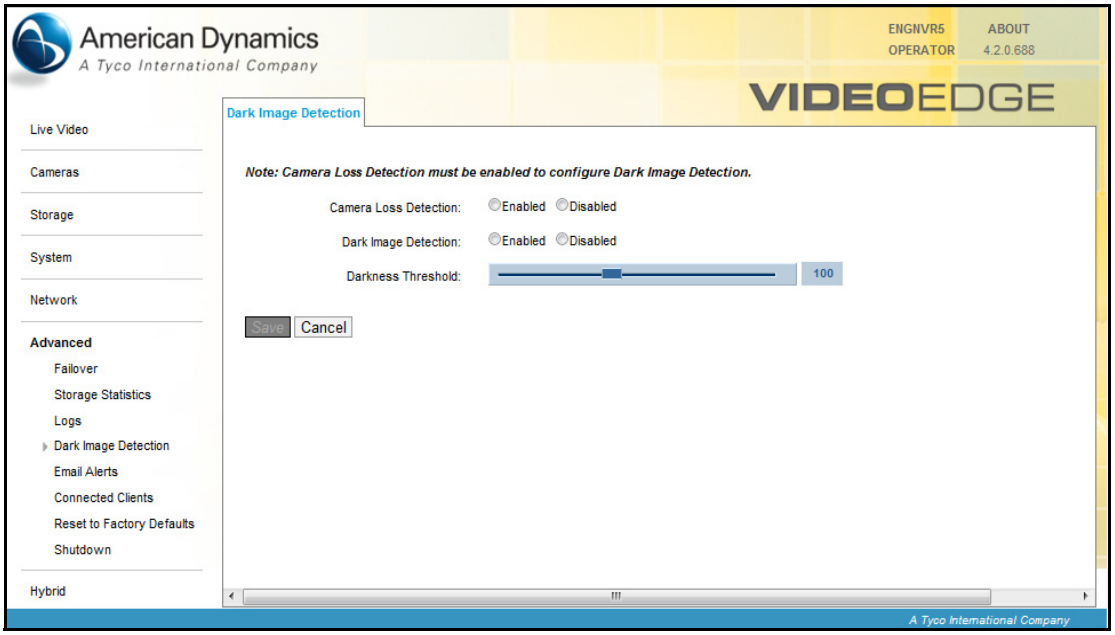
The NVR can perform a Dark Image Detection test on every camera in the network. You can use this test to determine if the NVR has a camera that is recording a very dark, or potentially black video. The test runs for each camera once a minute, it counts the number of pixels with intensity values less than the Darkness threshold which is defined in the Dark Image Detection page. The Darkness threshold can be set from 1 (darkest) to 255 (brightest), with a default setting of 80.

For example, with a Darkness threshold setting of 80, a pixel with RGB values of 70, 70, 70 is considered dark, while a pixel with RGB values of 70, 70, 81 is not considered dark. If 90% of all pixels are dark (have intensities less than the threshold you have set), then a 'Video Loss' alert is activated.

You can also enable Camera Loss Detection. If the camera goes offline a 'Video Loss' alert is triggered.

In victor client use the Activity Log page or the Reports feature to see if any cameras have generated any 'Video Loss' alert events.

**Figure 21-1 Dark Image Detection Page**



# Enable Dark Image Detection

Before Dark Image Detection can be enabled you must enable the Camera Loss Detection option. When dark image detection occurs, a “Video Loss” alert is activated. Both camera loss detection and dark image detection alerts can be viewed in the victor client Activity List or via the Reports feature.

## Procedure 21-1
## Enable Dark Image Detection

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Dark Image Detection**.<br>The Dark Image Detection page opens. |
| 3 | To enable Camera Loss Detection, click the **Enabled** option button. |
| 4 | To enable Dark Image Detection click the **Enabled** option button.<br>The area behind the option buttons changes to yellow indicating a change has been made. |
| 5 | To edit the Darkness Threshold use the slider to select the **Darkness Threshold** value.<br>The slider color changes to yellow indication a change has been made. |
| 6 | Click **Save**.<br>Confirmation messages display. |

**- End -**

# Enable/Disable Camera Loss Detection

When camera loss detection is enabled, a video loss alert is triggered when communication is lost between a camera and the NVR.

When camera loss detection is disabled, a video loss alert will not be triggered and the Dark Image Detection feature cannot be enabled.

## Procedure 21-2
## Enabling/Disabling Camera Loss Detection

| Step | Action |
|---|---|
| 1 | Select **Advanced**. |
| 2 | Select **Dark Image Detection**.<br>The Dark Image Detection page opens. |
| 3 | Click the **Enabled** option button to enable Camera Loss Detection.<br>Or |

Click the **Disabled** option button to disable Camera Loss Detection

The area behind the option buttons changes to yellow indicating a change has been made.

4 Click **Save**.

A confirmation message displays.

**- End -**

# Appendix A: Storage

## Overview

NVRs can require a tremendous amount of storage space depending on the number of cameras, codec, resolution, frame rates, recording modes, and the duration for which you want to preserve video recordings. At the outset of your use of the NVR system, you will need to have storage configured to record media data captured by video devices (cameras or encoders) connected to your NVRs. From time to time, you may find it necessary to replace or add a storage device to produce a greater capacity for video storage.

This section provides instructions for connecting NVRs to Fibre and iSCSI RAID devices then using them with the NVR. It is assumed that the storage device's Disk Groups (RAID set) and Virtual Disks (LUNs) have been properly configured and the device has been physically connected to the NVR. Use the operating system to mount any local storage device or any network storage device to the NVR.

## Storage Concepts

### iSCSI

- This standard is used to transmit data over local area networks (LANs), wide area networks (WANs) and can enable location-independent data storage and retrieval.
- A system that uses iSCSI requires an initiator. Initiators are iSCSI clients and they can either be in software or hardware.
- iSCSI does not require dedicated cabling; it can use existing switching and IP equipment. As a result, iSCSI is thought to be a low-cost alternative to Fibre Channel, which requires dedicated infrastructure.

### Fibre Channel

- Fibre Channel, or FC, is a gigabit-speed network technology primarily used for storage networking. It got its start in the supercomputer field, but has become the standard connection type for storage area networks (SAN) in enterprise storage.
- Fibre Channel Host Bus Adapters (HBAs) are available for all major open systems, computer architectures, and buses, for example, PCI. They are needed to connect a Fibre storage device to a server.

## Direct Attached Storage

- This term is used to differentiate non-networked storage from networking systems such as NAS and SAN.
- However, DAS cannot share information or space with other servers.
- DAS are usually connected via SCSI cables, along with a SCSI terminator.
- DAS can also be connected via eSATA or USB.

## Storage Types

- **JBOD** – Just a Bunch of Disks
- **RAID** – Redundant Array of Inexpensive Disks

### JBOD

- The JBOD storage configuration is a group of disks without any RAID features, depending on configuration in BIOS.
- In NVR systems, JBOD is rarely used with external devices.

### RAID

- An umbrella term for computer data storage schemes that distribute data across multiple disks for increased input/output performance and/or better reliability.
- Since RAID systems use multiple disks, they are often referred to as disk groups.
- Disk groups are also known as volumes or RAID arrays.
- There are different types of RAID configurations. Some of the best known configurations are RAID 0, 1, 5 and 1+0.
- Each configuration uses an approach to storage that can provide fault tolerance, additional availability of data, redundancy, additional performance, or more than one of these factors.

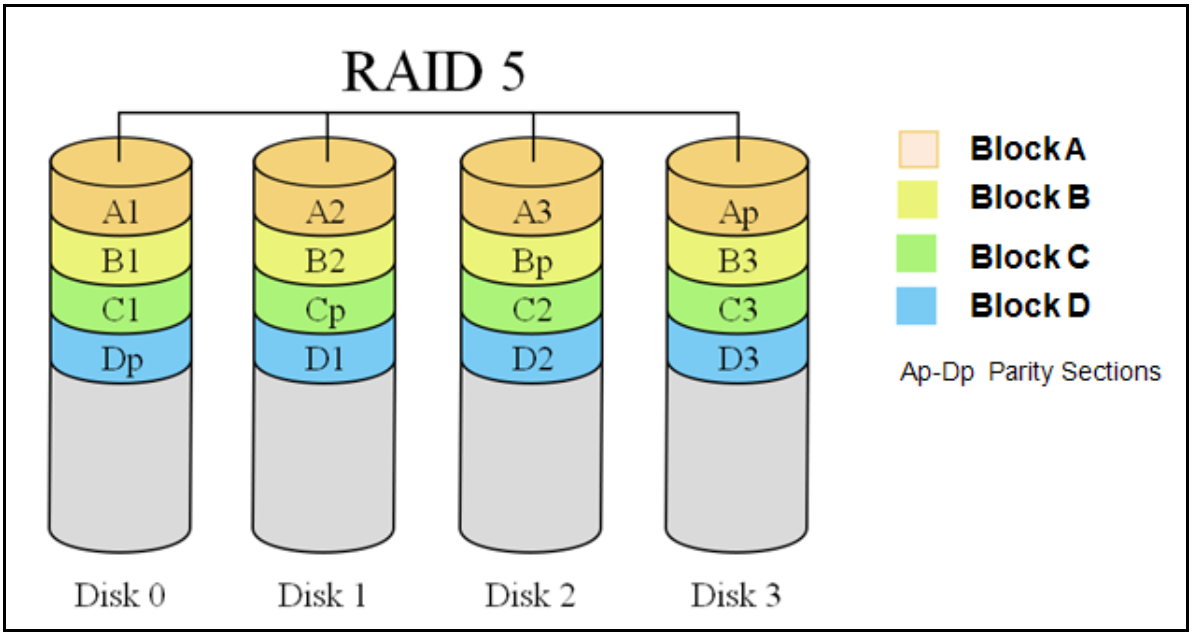
#### Key RAID Concepts

- **Mirroring** – Duplicating data to more than one disk.
- **Striping** – Splitting data across more than one disk.
- **Error Correction** – Storing redundant data so problems can be detected and possibly fixed.

#### Common RAID Types

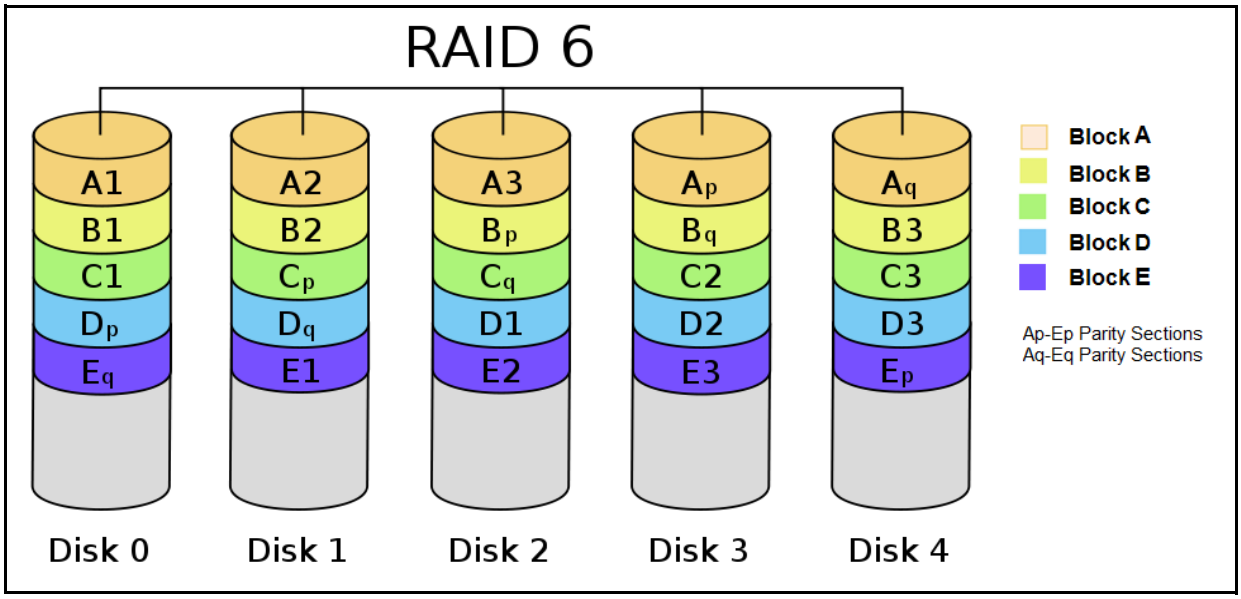
- **RAID 0** – Uses striping to provide extra performance and capacity but does not provide data protection (lack of mirroring or parity).
- **RAID 1** – Uses mirroring to provide 1:1 backup, which increases read performance or reliability at the expense of capacity. This configuration is often used with databases due to better transaction time and availability.
- **RAID 1+0** (or 10) – is a mirrored data set (RAID 1) which is then striped (RAID 0), hence the name “1+0”. A RAID 1+0 array requires a minimum of four drives – two mirrored drives to hold one half of the striped data, plus another two mirrored drives to hold the other half of the data. In LINUX, MD RAID 10 is a non-nested RAID type like RAID 1 that only requires a minimum of two drives and may give read performance on the level of RAID 0.
- **RAID 5** – Preserves against the loss of any one disk by combining the contents of three or more disks. However, the total storage capacity is reduced by one disk. This configuration is often used with VideoEdge because of RAID 5’s performance in situations where data transfers are I/O intensive (“RAID 5 Performance Benchmarks” The Server Company).

Figure 22-1 RAID 5




- **RAID 6** - Preserves against the loss of two disks failing at once by combining the contents of three or more disks. However, the total storage capacity is reduced by two disks.

Figure 22-2 RAID 6




## Virtual Disks (Logical Unit Numbers)

- A virtual disk represents an individually addressable (logical) SCSI device that is a partition of a physical SCSI device (target).
- Virtual disks are also known as volumes or LUNs.
- In enterprise-level systems, virtual disks usually represent segments of large RAID disk arrays.

# Storage Strategy

In order to properly configure an NVR, it is important to understand how much storage you will require and how to configure it to maximize the overall performance.

To configure storage on an NVR you must consider:

**1** Storage

- The type of storage to be used (Internal HDDs, iSCSI external storage, Fiber Optic external storage, USB external hard drives, etc).
- The storage configuration (RAID 0, RAID1, RAID 5, RAID 6, JBOD, etc).

**2** Cameras

- Total number of cameras.
- Type of cameras (make/model, resolution, codec, FPS, compression, recording mode).
- The file size of the camera's video stream that is to be recorded.

**3** The required recording retention period for stored video.

Below details some different storage usage examples and are compared to the NVR 4.1 storage model:

- **Example 1: Using a 20TB RAID set**

  **NVR 4.1**: 20TB RAID set is divided into 10 2TB logical volumes. There are **10 storage devices** seen on the NVR.

  **NVR 4.2.1**: 20TB RAID set can be added as 1 20TB volume. The NVR will recognise this as **1 storage device** that can be used for storage. Alternatively you can create 10 2TB logical partitions. The NVR will recognise this as **10 storage devices** that can be used for storage.

  **NVR 4.2.1 (Migrated from 4.1)**: 20 TB RAID set is still divided into 10 2TB logical volumes. Each 2TB volume is represented as 14 storage devices. The NVR will recognise this as **140 storage devices** that can be used for storage.

- **Example 2: Configuration Set up**

  **NVR 4.1**: Storage configuration is performed using the admin web GUI.

  **NVR 4.2.1**: Storage configuration is performed using Linux YaST/Partitioner.

  If you want to use the XFS file system for maximum throughput, additional file system options need to be configured. For Internal devices, you need to configure; **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m**. For external devices, including iSCSI and Fibre Optic, you need to configure; **nofail,rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m**.

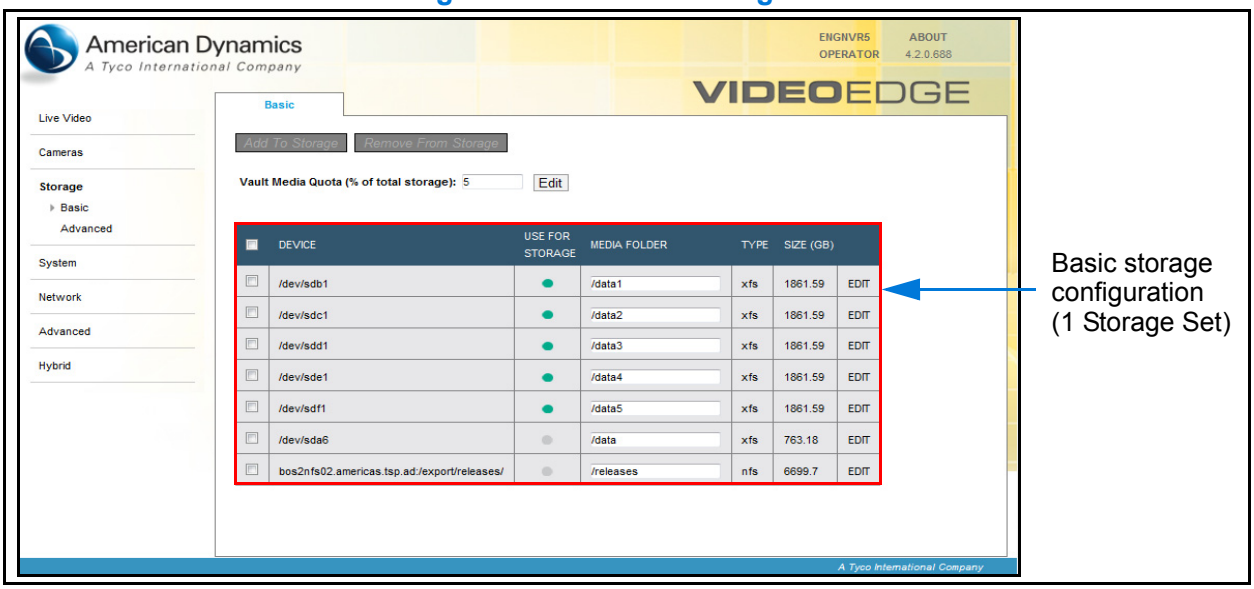
**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

# Understanding Storage Sets

The NVR uses a feature called Storage Sets. These are groups of storage devices and cameras. By default the NVR has one storage set - Storage Set 1. Initially the default storage set has all detected storage devices, their media folders and cameras assigned to it.

**Figure 22-3 Default Storage Set**




A Media Folder is a location on a device where media can be recorded to. Media stored in these folders can include video, audio and analytic media. You can only have one media folder per storage device partition or storage device, depending on your storage configuration. You can choose which media folders on devices are to be used for storage.

Video from the cameras assigned to a particular storage set will record to the media folders on the storage devices that are assigned to the same storage set.

You can easily create additional storage sets and configure them as required to optimize the disk performance, as media can be recorded to storage sets in parallel.

Each storage set must have at least one assigned media folder for storage. You can assign multiple media folders and cameras to a storage set. There is no limit to the number of storage sets you can create. It is recommended that you assign no more than 32 devices or cameras to a particular storage set. For example, if a NVR has a 50 camera licence, you could have the following storage set options:

**2 Storage Sets**

- Storage Set 1 = 25 CAMs record to first set of drive(s)
- Storage Set 2 = 25 CAMs record to second set of drive(s)

Or

- Storage Set 1 = 32 CAMs record to first set of drive(s)
- Storage Set 2 = 18 CAMs record to second set of drive(s)

**3 Storage Sets**

- Storage Set 1 = 10 CAMs record to first set of drive(s)

- Storage Set 2 = 20 CAMs record to second set of drive(s)
- Storage Set 3 = 20 CAMs record to third set of drive(s)

Or

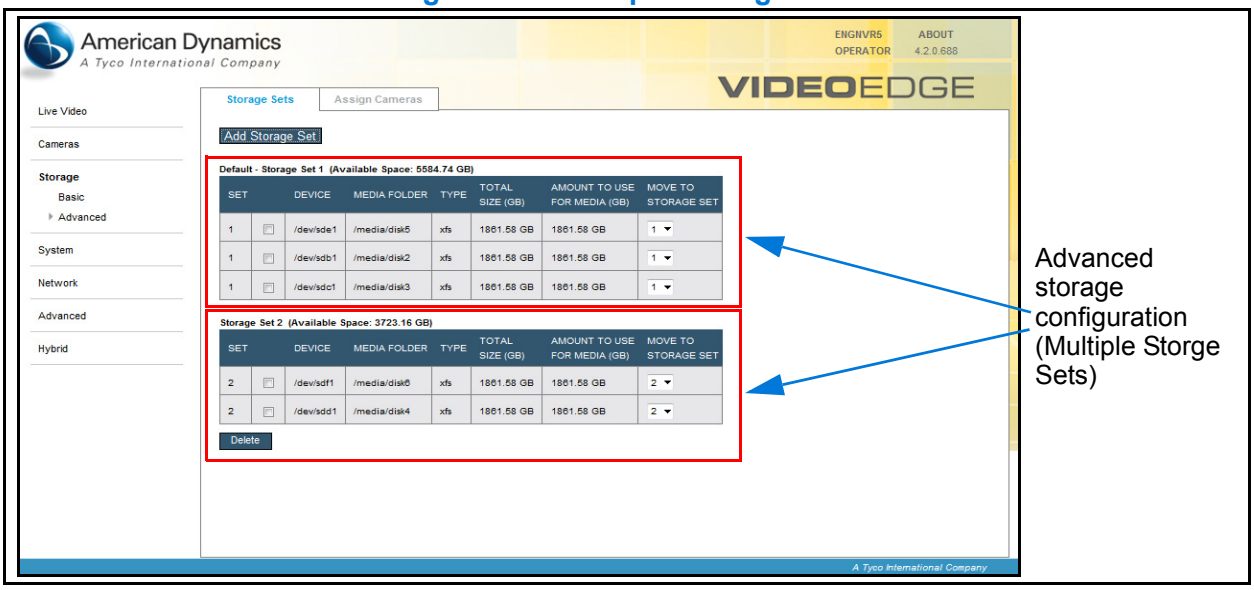
- Storage Set 1 = 16 CAMs record to first set of drive(s)
- Storage Set 2 = 17 CAMs record to second set of drive(s)
- Storage Set 3 = 17 CAMs record to third set of drive(s)

**Note**

1 The lower number of cameras per storage set, the higher achievable throughput. This is due to a lower total data rate required to record to each storage device.

2 High bit rate cameras (e.g. megapixel) should be spread across storage sets for load balancing.

**Figure 22-4 Multiple Storage Sets**




## Caution

Avoid assigning Virtual Disks from the same Disk Group to different storage sets. If this is done, there is a high probability that continuous disk thrashing will cause the storage device to lock up and cause undesirable results to the NVR.

# Calculating Storage Requirements

You need to have enough storage space to fulfil your video recording requirements without data being culled unnecessarily. To ensure you do have enough storage it is important to carefully calculate your storage requirements.

### Procedure 22-1
### Calculating Storage Requirements

| Step | Action |
|---|---|
| 1 | Determine the quantity of Edge Devices and Anticipated Settings Make/Model, Codec/Rez/FPS/Compress, Activity, Record Hours. |
| 2 | Calculate the Data Rate for each device using Vendor Calculators.<br>For example;<br>• AD http://www.americandynamics.net/calculators/calc_4C_VideoEdge_IP_Encoder.html<br>• Axis http://www.axis.com/products/video/design_tool/calculator.htm<br>• Sony http://pro.sony.com/bbsccms/ext/cat/camsec/cameraCalc3/HTML/NTSC_Calculator.html |
| 3 | Enter the required information into the NVR Storage Requirement Calculator.<br>http://www.americandynamics.net/calculators/Calc_NVR_Storage_Requirement.html |
| 4 | The calculator output provides the **Total Storage for All Cameras** and the **Total Bandwidth for All Cameras**.<br>You may need to lower the camera count per NVR to meet network and storage requirements when dealing with many cameras, large resolution, or retention. |
| 5 | The maximum cameras per NVR based on current NVR Bundle Server spec:<br>• 128 Cameras with a total network bandwidth of 400Mbps maximum with continuous recording on either Fibre or iSCSI storage.<br>• 64 Cameras with a total network bandwidth of 400Mbps maximum with motion based recording on either Fibre or iSCSI storage. |

**- End -**

# Overview of AD Fibre RAID Storage (FRS/FES)

Fibre RAID Storage is an NVR extended storage device acting as a Fibre Direct-Attached Storage (DAS) or iSCSI device.

As a Fibre device, a Fibre Host Bus Adapter (HBA) must be installed in the NVR and uses Fibre Optic cable connection.

As an iSCSI device, 3rd Gigabit Ethernet NIC must be installed in the NVR and uses CAT 5e/6 Ethernet connection. This is already installed in the NVR 4.2.1 servers.

# Second generation American Dynamics iSCSI and Fibre RAID Storage

The second generation American Dynamics iSCSI and Fibre RAID Storage solutions are designed for high-performance recording devices. They are secure and highly scalable storage solutions that provide SAN storage for virtually any network and application.

The new Rack Mount models are available in a variety of configurations and capacities. There are iSCSI RAID, 4Gb Fibre RAID, and Expansion models which have been uniquely designed to utilize the same 3U chassis. These storage solutions come standard with redundant power supplies and fans, and nearly every component is hot-swappable, including sixteen lockable hot-swap drives. An optional battery backup module is also available for the iSCSI and FibreRAID units.

# Storage Strategy for FRS/FES RAID Device

## Recommendations

- The FRS/FES supports a maximum of eight (8) Disk Groups (aka RAID sets).
- Each Disk Group can be “carved up” into one or more Virtual Disks (aka Volumes or LUNs). It is recommended to try to maximize each virtual disk size.
- It is recommended that Virtual Disks from a single Disk Group are all assigned to the same NVR Storage Set. This will eliminate the possibility of unnecessary disk thrashing caused when the same set of physical disks (DGs) are being used by different sets of cameras (aka Storage Sets).
- Verify that you have the latest firmware patch or upgrade for your controller.
- Make sure to leave a minimum of a 2U space between storage units.
- Start the camera’s recording after all the drives have been formatted and their status is “Normal”.

# Connecting Additional Storage Devices

## Connecting NVR to FRS/FES Using Fibre

Before configuring external storage you must stop NVR Services. Refer to Procedure 16-2 Stop NVR Services on page 170.

Once you have connected and configured external storage devices, you must restart the NVR Services. Refer to Procedure 16-1 Restart NVR Services on page 170.

### Procedure 22-2
### Connecting NVR to FRS/FES Using Fibre

| Step | Action |
|---|---|

1. Power OFF the NVR and install the Fibre HBA Kit (PCI-e). Connect the AD Fibre RAID Storage to the NVR.
2. Reboot the NVR and log in to the NVR desktop as the Root User.
3. Select **Computer**.
4. Select **YaST** from the System menu.

   The Control Center opens.
5. Select **Partitioner**.

   A warning message opens.
6. Click **Yes**.

   The Expert Partitioner window opens.
7. Expand the **Hard Disks** menu.
8. Right-click the new storage device from the list of hard disks, then click **Edit**.
9. Click **Add**.

   The Add Partition window opens.
10. Set the new partition size. You can select **Maximum Size**, **Custom Size** and enter a value, or select **Custom Region** where you can choose the disk cylinders for the partition.

    **Note**

    In order to use a disk partition for storage it must meet the minimum storage capacity requirements, 10GB.
11. Click **Next**.
12. Ensure the **Format partition** option button is selected. Select **XFS** from the **File system** dropdown menu.
13. Select the **Mount Partition** option button.
14. Enter the **Mount Point** for the disk.
15. Select the **Fstab Options...** button.
16. Enter **nofail,rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

    **Note**

    **nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.
17. Click **OK**.

    **Note**

    Each mount point should have a unique name, however, it is good practise to use a folder structure naming convention, for example,
    mount point 1: /data/media1,
    mount point 2: /data/media2,
    mount point 3: /data/media3, etc.
18. Click **Finish**.

19 Click **Next**.

The Expert Partitioner Summary displays a list of the changes that will be made to the NVR partitions.

20 Click **Finish**.

The Perform Installation page opens and the disk partition for the new storage device is created.

21 Configure the NVR to allow the new disk to be used for storage:

**a** Open a web browser.

**b** Enter the IP address of the NVR into the **URL** field.

The NVR login dialog box opens.

**c** Enter the Administrators **User name** and **Password**.

User name: **admin**

Default Password: **VIDEO!edge23**

**d** Select **Storage** from the main menu.

**e** Select **Basic**.

The Basic Storage Configuration page opens.

**f** Locate the new storage device in the summary table and select the checkbox in the storage device record.

**g** Click **Add to Storage**.

22 The connection and configuration of a fibre storage device is complete. The fibre device can now be used to store media from the NVR.

**- End -**

## Connecting NVR to FRS/FES Using iSCSI

Before configuring external storage you must stop NVR Services. Refer to Procedure 16-2 Stop NVR Services on page 170.

Once you have connected and configured external storage devices, you must restart the NVR Services. Refer to Procedure 16-1 Restart NVR Services on page 170.

### Procedure 22-3
### Connecting NVR to FRS/FES Using iSCSI

| Step | Action |
|---|---|

1 Power OFF the NVR and install the iSCSI NIC Card (LAN3) into correct and compatible slot.

2 Connect the iSCSI RAID Storage device to a switch or directly to NVR LAN3 to ensure that it is accessible.

3 Open a web browser.

4 Enter the IP address of the iSCSI storage device into the **URL** field.

The web configuration interface for the iSCSI storage device opens.

5 Enter the **User name**.

**Note**

The default User name is **admin**.

6 Enter the **Password**.

**Note**

The default Password is **admin**.

7 Set up the NIC IP settings for the iSCSI port:

**a** Select **iSCSI Configuration** from the iSCSI RAID Rack menu.

The iSCSI Configuration sub-menu items are displayed.

**b** Select **NIC**.

A summary of all NICs available in the storage device are displayed.

**c** Check the values in the **Link** fields. If the value is **Up**, this represents that a cable is present connecting the storage device and the NVR. This is the NIC you need to configure.

**d** Select the dropdown list in the **Name** field for the NIC with the **Link** field value set to **Up**.

**e** Select **IP Settings for iSCSI ports** from the dropdown list.

The NIC IP settings page opens.

**f** If required, edit the Static **Address**, **Mask** and **Gateway**.

**Note**

If there are no DHCP settings available these fields will contain the default values, Address: 10.10.10.20, Mask: 255.255.255.0 and Gateway: blank.

**g** Click **Confirm**.

The NIC settings page closes and the NIC summary details are displayed.

8 Create a Node to associate the storage NIC with an NVR port:

**a** Select **Node** from the iSCSI Configuration sub-menu.

**b** Click **Create**.

**c** Enter a **Name** for the Node.

**d** Select the type of **Authentication** from the dropdown list. The default is **None**.

**Note**

Select **CHAP** to use a password for data transfer.

**e** Select the checkbox for the required **Portal.** This is the portal which contains the NIC IP address.

**f** Click **Confirm**.

**9** Assign the required Virtual Drives a LUN:

**Note**

The Virtual Drives are pre-configured on the storage device.

**a** Select **Volume configuration** from the iSCSI RAID Rack menu.

The Volume configuration menu expands.

**b** Select **Logical Unit**.

**c** Click **Attach**.

**d** Select the virtual disk from the **VD** dropdown list.

**e** Select the LUN from the **LUN** dropdown list.

**f** Click **Confirm**.

The Virtual Disk is assigned to the LUN and appears in the Logical unit summary table.

**g** Repeat Steps c to f to assign all the required Virtual Disks to a LUN.

**10** Configure the Network Settings on the NVR:

**a** Log in to the NVR desktop as the Root user.

**b** Select **Computer**.

**c** Select **YaST** from the System menu.
The Control Center opens.

**d** Select **Network Settings** from the Network Devices section.

The Initializing Network Configuration window displays momentarily and the Network Settings page opens.

**e** Select the **Overview** tab.

**f** Select the storage network card.

**g** Click **Edit**.

**h** Select the **Statically assigned IP Address** option button.

**i** Enter the **IP Address**.

**j** Enter the **Subnet Mask**, 255.255.255.0.

**k** Enter the **Hostname**.

**l** Click **Next**.

**m** Click **OK**.

**n** Close the Network Settings window.

**11** Test the network connection between the NVR and the iSCSI storage device:

**a** Double-click **GNOME Terminal** on the desktop.

The Terminal window opens.

**b** Type ping followed by the IP address of the storage device, for example, ping 192.168.8.1. Press **[Enter]**.

**Note**

If the connection is unsuccessful, a ‘Destination Host Unreachable’ message is displayed. Check the connections and network settings and retry.

**c** Close the Terminal window.

**12** Connect the storage device using the iSCSI initiator:

**a** In the Control Center, enter iSCSI into the Filter field.

**b** Select **iSCSI Initiator**.

The iSCSI Initiator Overview window opens. The Discovered Targets tab displays the discovered storage devices. At this stage the value in the **Connected** field is **False**.

**c** Select the **Service** tab.

**d** Select the **When Booting** Service Start option button.

**e** Select the **Discovered Targets** tab.

**f** Click **Discovery**.

**g** Enter the **IP Address**.

**Note**

This is the IP Address of the storage device.

**h** Enter the **Port**. The default port number is **3260**.

**i** Select the **No Authentication** checkbox.

**j** Click **Next**.

The iSCSI storage device is listed in the Discovered Targets table.

**k** Select the storage device and click **Log In**.

**l** In the **Startup** field select **Automatic** from the dropdown list.

**m** Click **Next**.

The value in the **Connected** field has been updated to **True**. This means the storage device is connected to the NVR.

**n** To confirm the storage session is connected, log into the storage web interface (see Steps 3 to 6), select the **iSCSI configuration** in the menu, select **Session** and ensure the session is connected with the correct initiator name.

**13** Mount the storage drive on the NVR:

**a** Select **Partitioner** from the System section in the Control Center.

A warning message opens.

**b** Click **Yes**.

The Expert Partitioner window opens.

**c** Expand the **Hard Disks** menu.

**d** Select the new storage device from the list of hard disks.

Information about the storage partitions on the disk is displayed in the Partitions tab.

**e** Click the **Expert** dropdown list.

**f** Select **Create New Partition Table** from the dropdown.

A message box opens.

**g** Select the **GPT** partition type.

**h** Click **OK**.

A message box opens to confirm that you are sure you want to create a new partition.

i Click **Yes**.

j Click **Add**.

The Add Partition window opens.

k Set the new partition size. You can select **Maximum Size**, **Custom Size** and enter a value, or select **Custom Region** where you can choose the disk cylinders for the partition.

**Note**

In order to use a disk partition for storage it must meet the minimum storage capacity requirements, 10GB.

l Click **Next**.

m Ensure the **Format partition** option button is selected. Select **XFS** from the **File system** dropdown menu.

n Select the **Mount Partition** option button.

o Enter the **Mount Point** for the disk.

p Select the **Fstab Options...** button.

q Enter **nofail,rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

r Click **OK**.

**Note**

Each Mount Point should have a unique name, however, it is good practice to use a folder structure naming convention, for example,
mount point 1: /data/media1,
mount point 2: /data/media2,
mount point 3: /data/media3, etc.

s Click **Finish**.

t Click **Next**.

The Expert Partitioner Summary displays a list of the changes that will be made to the NVR partitions.

u Click **Finish**.

The Perform Installation page opens and the disk partition for the new storage device is created.

**14** Configure the NVR to allow the new disk to be used for storage:

a Open a web browser.

b Enter the IP address of the NVR into the **URL** field.

The NVR login dialog box opens.

c Enter the Administrators **User name** and **Password**.

User name: **admin**
Default Password: **VIDEO!edge23**

**d** Select **Storage** from the main menu.

**e** Select **Basic**.

The Basic Storage Configuration page opens.

**f** Locate the new storage device in the summary table and select the checkbox in the storage device record.

**g** Click **Add to Storage**.

**15** The connection and configuration of an iSCSI storage device is complete. The iSCSI storage device can now be used to store media from the NVR.

**- End -**

# Appendix B: Web Client Pre-configuration

## Overview

For a client PC to communicate with the NVR and its web interface there are basic Windows configuration settings and software that must be in place.

## Prerequisite Software

There are several software components that need to be installed on the client PC before you can access a NVR using the Web Interface.

Each prerequisite software component can be downloaded from their respective company websites.

When the software items have been downloaded and saved to your computer you can double-click the software packages and follow the installation instructions to complete the software installation process.

The correct drivers must also be installed for the PC's hardware, for instance, it is extremely important to load the manufacturers most current driver for a video card. If the correct drivers are NOT installed, you may get undesired effects and/or damage the PC and its hardware.

The prerequisite software that needs to be installed are:

- Microsoft Windows Internet Explorer (Version 8 or 9).
- Java 6 and above - Used by the web client user interface.
- QuickTime 7.7 and above.
- (Optional) Adobe® Reader® X and above - Used to read documentation in PDF format.

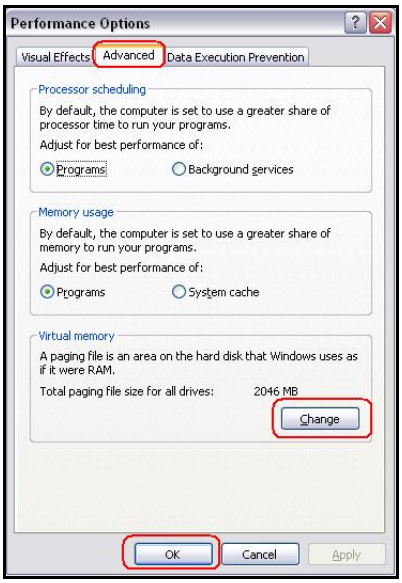
## Configuring the Paging File

You can improve the display of streaming video by setting the Paging File size to be managed by windows. This is the default setting. If you have modified this setting and you are experiencing any problems viewing video via the NVR Web Interface, you can perform the following steps to restore this setting.

## Procedure 23-1
## Configuring the Paging File (XP)

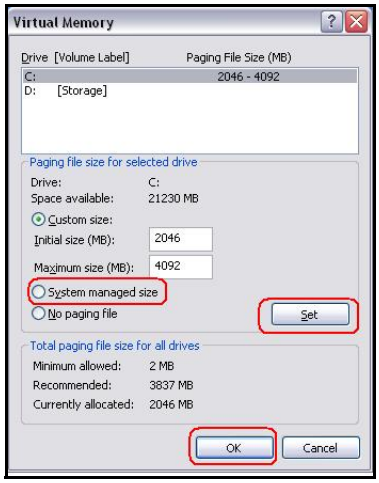
| Step | Action |
|---|---|
| 1 | Click **Start** in the Windows taskbar. |
| 2 | Right-click **My Computer** and select **Properties**. |
| 3 | Select the **Advanced** tab. |
| 4 | In the **Performance** section, click **Settings**. |
| 5 | Select the **Advanced** tab. |
| 6 | In the **Virtual Memory** section, click **Change**. |

**Figure 23-1 Change Virtual Memory**


Performance Options
Visual Effects
Advanced
Data Execution Prevention
Processor scheduling
By default, the computer is set to use a greater share of processor time to run your programs.
Adjust for best performance of:
Programs
Background services
Memory usage
By default, the computer is set to use a greater share of memory to run your programs.
Adjust for best performance of:
Programs
System cache
Virtual memory
A paging file is an area on the hard disk that Windows uses as if it were RAM.
Total paging file size for all drives:
2046 MB
Change
OK
Cancel
Apply

| | |
|---|---|
| 7 | In the **Paging file size for selected drive** section, select **System managed size** and click **Set**. |

**Figure 23-2 Selecting System Managed Size**




**8** Click **OK**.

If the System prompts you to reboot the PC, follow the reboot prompts.

**- End -**

## Procedure 23-2
## Configuring the Paging File (Windows 7)

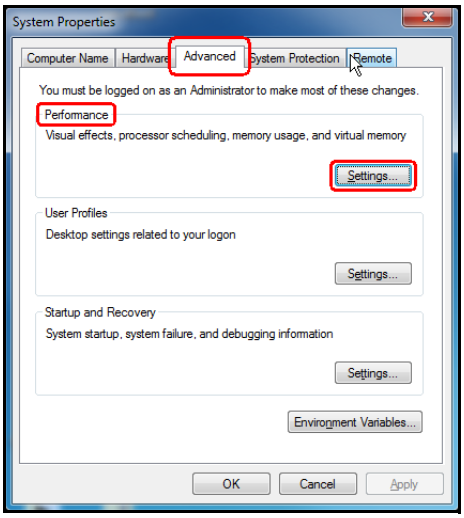
| Step | Action |
|---|---|

**1** Click **Start** in the Windows taskbar.

**2** Right-click **My Computer** and select **System Properties**.

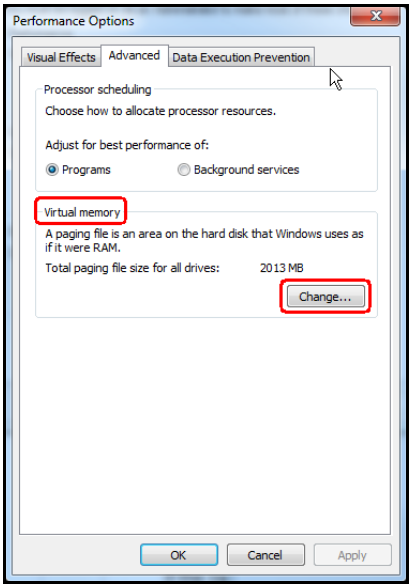
**3** Select **Advanced System Settings**.

**4** On the **Advanced** tab, in the **Performance** section, click **Settings**.




**5** Select the **Advanced** tab.

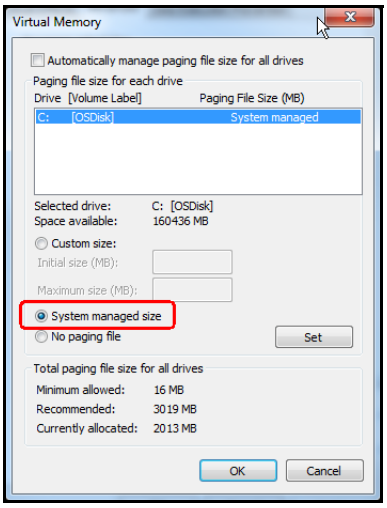
6 In the **Virtual Memory** section, click **Change**.




7 (Optional) Deselect **Automatically manage paging file size for all drives**.

The **Paging file size for selected drive** settings become available to edit.

8 In the **Paging file size for selected drive** section, select **System Managed Size** and click **Set**.




9 Click **OK**.

If the System prompts you to reboot the PC, follow the reboot prompts.

**- End -**

# Setting QuickTime Preferences

After you install QuickTime on the PC that you will use to access the NVR Web Interface, you need to adjust QuickTime Preferences if you wish to view video in a QuickTime pop-out window. The

sections below outline how to set the preferences depending on whether you are using the Windows XP or Windows 7 operating system.

## Setting QuickTime Preferences (XP)

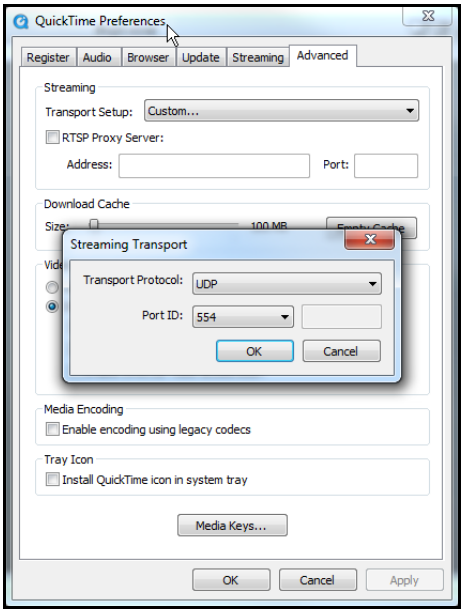
The QuickTime preferences you need to set when using Windows XP are:

- Set QuickTime to use UDP port 554.

### Procedure 23-3
### Set QuickTime Preferences

| Step | Action |
|---|---|
| 1 | Open a QuickTime window. |
| 2 | Select **Edit** > **Preferences** > **QuickTime Preferences** from the menus. |
| 3 | Select the **Advanced** tab. |
| 4 | In the **Transport Setup** dropdown menu, select **Custom**.<br>The Streaming Transport dialog box opens. |

**Figure 23-3 Streaming Transport dialog box**




| | |
|---|---|
| 5 | Select **UDP** from the **Transport Protocol** dropdown. |
| 6 | Select **554** as the **Port ID**. |
| 7 | Click **OK**. |
| 8 | Click **OK**.<br>You can close the QuickTime viewer by selecting **File** > **Exit**. |

**- End -**

# Setting QuickTime Preferences (Windows 7)

If you are accessing the NVR Web Interface from a Windows 7 PC, you must adjust several settings so that QuickTime can properly display NVR video:

- Turn off Windows Firewall
- Turn off Internet Security Protect mode
- Enable **Download unsigned Active X Controls**

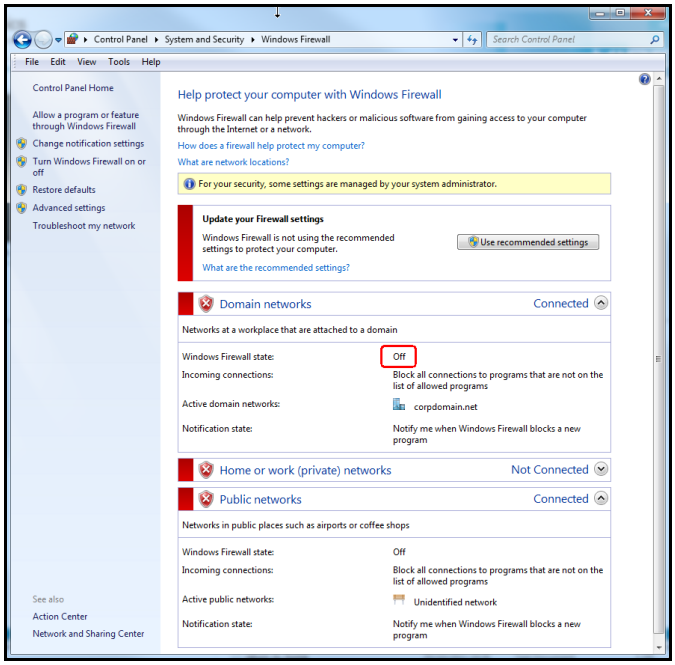
## Procedure 23-4
## Configure Settings for QuickTime Use on Windows 7

| Step | Action |
|---|---|

**1** Navigate to **Start** > **Control Panel** > **System and Security** > **Windows Firewall**.

**2** Verify that Windows Firewall is **Off** (turn it off if it is set to On).

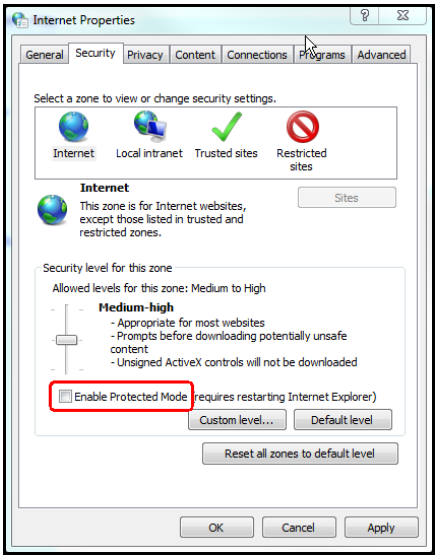
**Figure 23-4 Windows Firewall Settings**


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
File Edit View Tools Help
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
Help protect your computer with Windows Firewall
Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.
How does a firewall help protect my computer?
What are network locations?
For your security, some settings are managed by your system administrator.
Update your Firewall settings
Windows Firewall is not using the recommended settings to protect your computer.
Use recommended settings
What are the recommended settings?
Domain networks
Connected
Networks at a workplace that are attached to a domain
Windows Firewall state:
Off
Incoming connections:
Block all connections to programs that are not on the list of allowed programs
Active domain networks:
corpdomain.net
Notification state:
Notify me when Windows Firewall blocks a new program
Home or work (private) networks
Not Connected
Public networks
Connected
Networks in public places such as airports or coffee shops
Windows Firewall state:
Off
Incoming connections:
Block all connections to programs that are not on the list of allowed programs
Active public networks:
Unidentified network
Notification state:
Notify me when Windows Firewall blocks a new program
See also
Action Center
Network and Sharing Center

**3** Navigate to **Start** > **Control Panel** > **Network and Internet** > **Internet Options**.

**4** Select the **Security** tab and deselect the **Enable Protected Mode** check box.

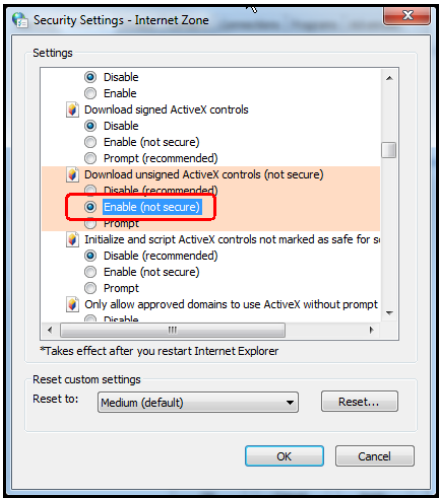
## Figure 23-5 Internet Properties Security Settings




5 Click **Custom Level**.

6 Scroll down the **Settings** list to **Download unsigned ActiveX Controls** and select **Enable**.

## Figure 23-6 Custom Security Settings




7 Click **OK**.

**- End -**

# Appendix C: Networking Troubleshooting

## Overview

If your client PC is unable to connect with the NVR, you will need to troubleshoot your difficulties. This Appendix covers two common network problems:

1. Your client PC has not been assigned an IP address (or addresses). Without an address, your NVR cannot communicate with the client.
2. Your client PC has an IP address but cannot reach the NVR. There are some basic tools for checking network connectivity: ipconfig /all, ping, and tracert.

This appendix can help you learn more about your network problems, and lead to solutions via procedural information for both Windows XP and Windows 7. However, American Dynamics strongly recommends that you do not attempt to solve network problems yourself unless you have training in networking. If the Troubleshooting procedures in this Appendix do not solve your networking problems, you should contact your Network Administrator for assistance.

### Table 24-1 Network Troubleshooting

| This problem... | May be caused by... | Check or do this... |
|---|---|---|
| Your Client PC cannot access any network device, including the NVR. | Your Client PC may not have an IP address assigned. | See Assigning an IP Address to a Client PC. |
| Your Client PC has an IP address but cannot reach the NVR. | Your Client PC may not be connected to the network. | Use the basic tools for checking network connectivity. Start by using **ipconfig /all** to determine if networking on your Client PC is configured. See Troubleshooting with the IPconfig /All Command. |
| | Your Client PC may not be able to reach the NVR or a network device such as a switch or router. | Use the **ping** command to determine whether you can reach the NVR or another known network device such as a router, a switch or another Client PC. See Troubleshooting with the Ping Command |
| | Your Client PC can connect to the network and ping some devices successfully, but may not be able to connect to the NVR. | Use the **tracert** command to determine if your communication with the NVR failing or timing out with another network device along the communications path. See Troubleshooting with the Tracert Command. |
| | Your Client PC can trace a route successfully to the NVR but still cannot connect to the NVR Web Interface. | Check to make sure that the NVR is operating correctly. |
| | | Can you use another Client PC to connect to the NVR Web Interface? |
| | | If no Clients can connect to the NVR Web Interface, the NVR's Web Server might not be running correctly. Reboot the NVR to restart the Web Server. When the NVR is running again, attempt to connect your Client PC again. |

# Assigning an IP Address to a Client PC

If you cannot access any network device and have no known hardware problems, your client PC may not have an IP address. In this section, you will check if to see if your PC has an address and add one if necessary. If you are unable to configure an IP address using these procedures, contact your network administrator.

## Procedure 24-1
## Assigning an IP Address to a Client PC (Windows XP)

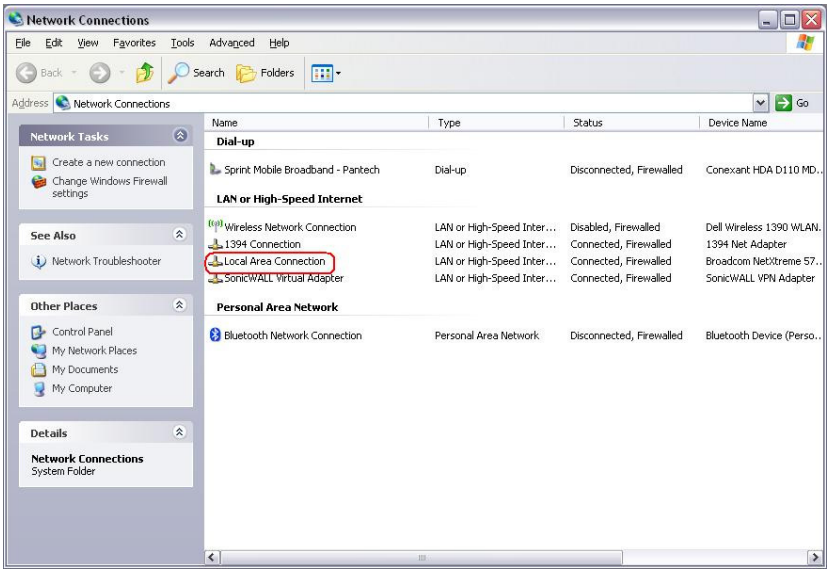
| Step | Action |
|---|---|
| 1 | Click **Start** in the Windows taskbar. |
| 2 | Mouse-over **My Network Places** and right-click. |
| 3 | Select **Properties**. |

Networks Connections screen displays.

**Figure 24-1 Selecting Properties of My Network Places.**

4 Locate your **Local Area Connection**.

**Figure 24-2 Network Connections**


Network Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network Connections
Go
Network Tasks
Create a new connection
Change Windows Firewall settings
See Also
Network Troubleshooter
Other Places
Control Panel
My Network Places
My Documents
My Computer
Details
Network Connections
System Folder
Name Type Status Device Name
Dial-up
Sprint Mobile Broadband - Pantech Dial-up Disconnected, Firewalled Conexant HDA D110 MD..
LAN or High-Speed Internet
Wireless Network Connection LAN or High-Speed Inter... Disabled, Firewalled Dell Wireless 1390 WLAN.
1394 Connection LAN or High-Speed Inter... Connected, Firewalled 1394 Net Adapter
Local Area Connection LAN or High-Speed Inter... Connected, Firewalled Broadcom NetXtreme 57..
SonicWALL Virtual Adapter LAN or High-Speed Inter... Connected, Firewalled SonicWALL VPN Adapter
Personal Area Network
Bluetooth Network Connection Personal Area Network Disconnected, Firewalled Bluetooth Device (Perso..

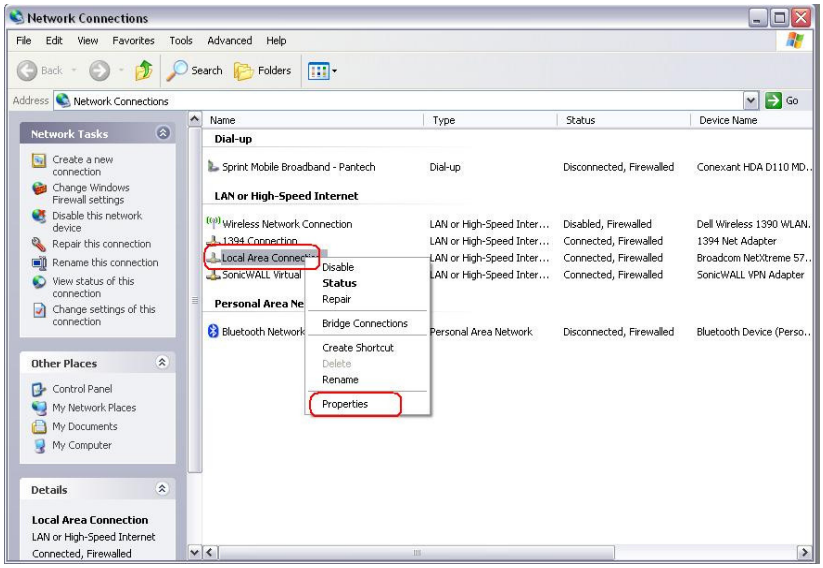
**Local Area Connection** refers to the primary NICs that is on the client PC.

5 Right-click **Local Area Connection**.

6 Select **Properties**.

The Local Area Connection Properties pop-up displays.

**Figure 24-3 Local Area Connection Properties.**

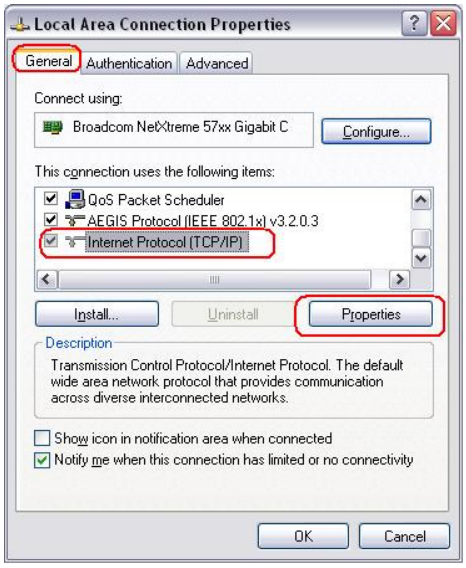



**7** Under the **General** tab, and in the section labeled **This connection uses the following items**, scroll down until you see **Internet Protocol (TCP/IP)** and highlight it.

**8** Click **Properties**.

The **Internet Protocol (TCP/IP) Properties** pop-up displays.

**Figure 24-4 Internet Protocol (TCP/IP) Properties.**




**9** Select the **General tab**. It provides two options for assigning an IP address to the PC:

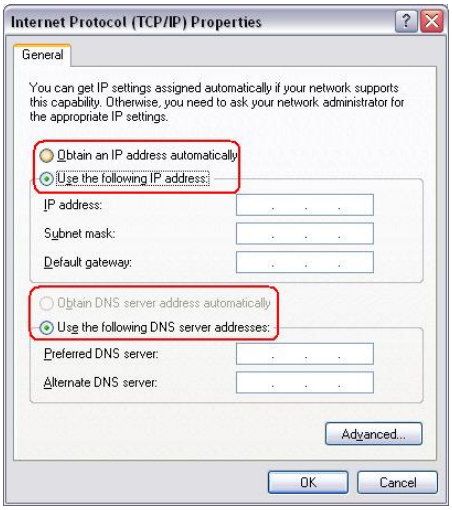
- **Obtain an IP address automatically** - When this option is selected, the client PC will obtain its IP address from a Dynamic Host Configuration Protocol (DHCP) server. The IP address will change every time the machine boots up.
- **Use the following IP address** - Select this option if you want to manually configure the TCP/IP settings. This option is strongly recommended because

you can specify the IP address, which makes it easier to do network troubleshooting should the need arise.

**10** This dialog box also provides two options for assigning a DNS address. You may or may not need a DNS address depending on the network. Consult your network administrator for more information.

- **Obtain DNS server address automatically** - Receives the DNS server address from a DHCP server.
- **Use the following DNS server addresses** - Allows you to add the DNS server's IP address(es) by hand.

**Figure 24-5 IP Addressing.**


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

**11** Click **OK** to close the **Internet Protocol (TCP/IP) Properties** pop-up.Click **OK** again to close the **Local Area Connection Properties** pop-up.

**12** Attempt again to communicate to the network from your Client PC (For example, open your internet browser to see if you can reach a website). If you still cannot access the network, refer to Troubleshooting Network Connections on page 252.

**- End -**

## Procedure 24-2
## Assign an IP Address to a Client PC (Windows 7)

| Step | Action |
|---|---|

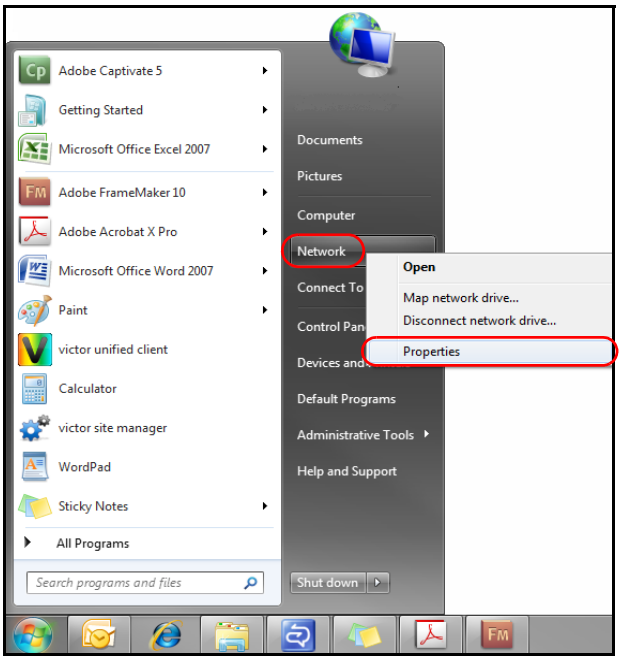
**1** Click **Start** in the Windows taskbar.

**2** Mouse-over **Network** and right-click.

**3** Select **Properties**.

The Network and Sharing Center opens.

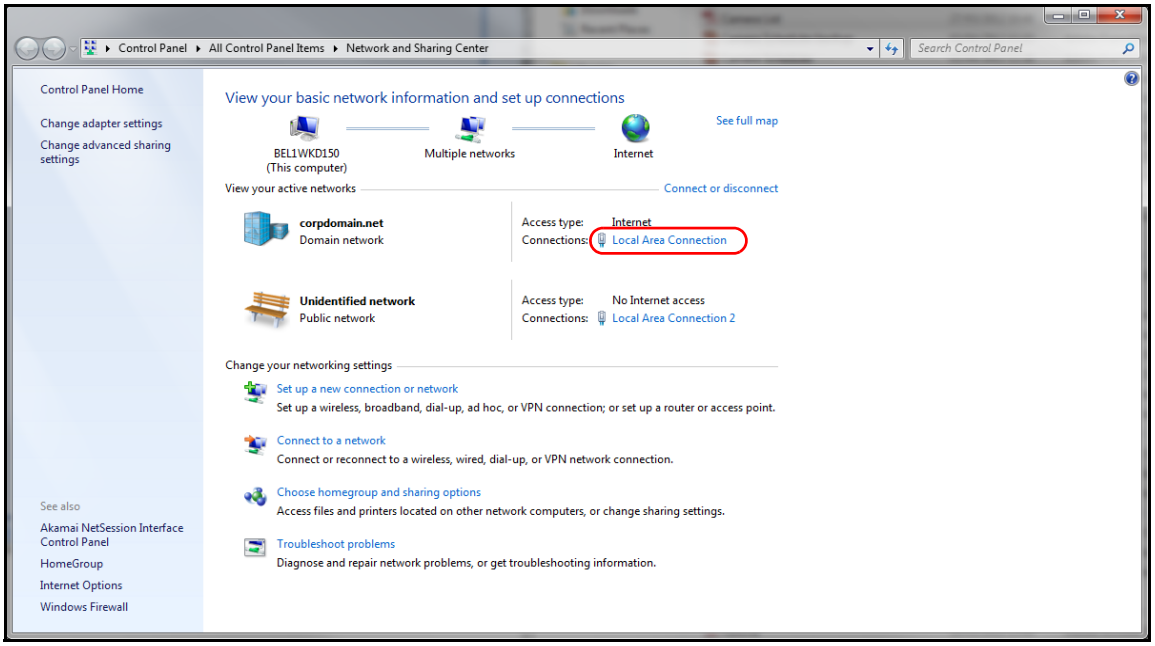
### Figure 24-6 Selecting Network Properties




**4** Select the primary **Local Area Network**.

The Local Area Connection Status pop-up displays.

### Figure 24-7 Network Connections


Control Panel ▸ All Control Panel Items ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
BEL1WKD150
(This computer)
Multiple networks
Internet
View your active networks
Connect or disconnect
corpdomain.net
Domain network
Access type: Internet
Connections: Local Area Connection
Unidentified network
Public network
Access type: No Internet access
Connections: Local Area Connection 2
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Akamai NetSession Interface Control Panel
HomeGroup
Internet Options
Windows Firewall

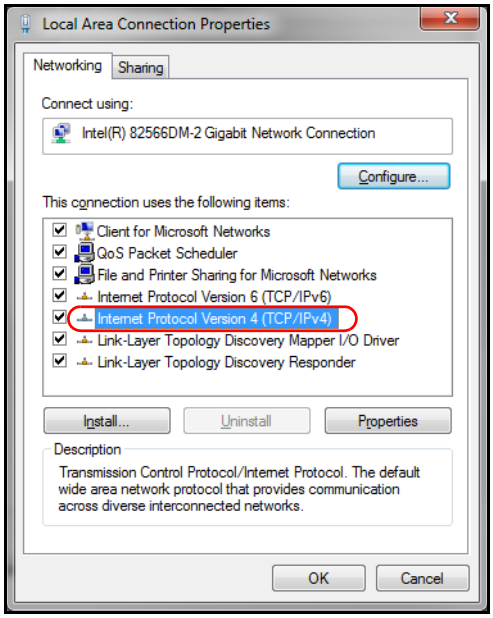
**5** Select **Properties**.

The Local Area Connection Properties pop-up displays.

**6** Under the Networking tab double-click on **Internet Protocol Version 4 (TCP/IPv4)**.

The Internet Protocol Version 4 (TCP/IPv4) Properties pop-up displays.

**Figure 24-8 Local Area Connection Properties**



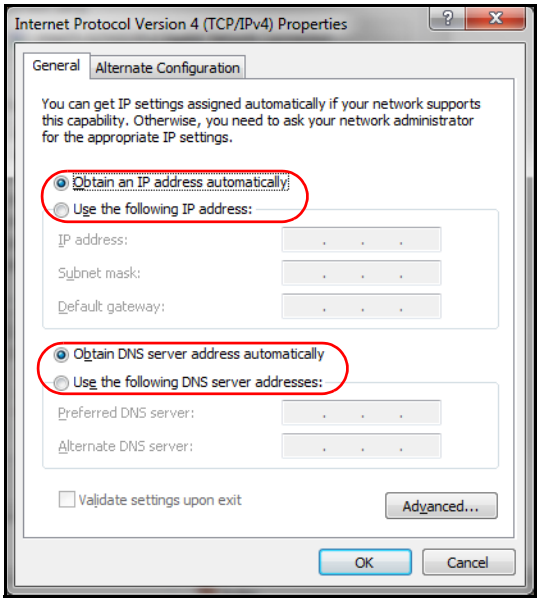

**7** Select the **General Tab**. It provides two options for assigning an IP address to the PC:

- **Obtain an IP address automatically** - When this option is selected, the client PC will obtain its IP address from the Dynamic Host Configuration Protocol (DHCP) server. The IP address will change every time the machine boots up.
- **Use the following IP address** - Select this option if you want to manually configure the TCP/IP settings. This option is strongly recommended because you can specify the IP address, which makes it easier to do network troubleshooting should the need arise.

**8** This pop-up menu also provides two options for assigning a DNS address. You may or may not need a DNS address depending on the network. Consult your network administrator for more information.

- **Obtain DNS server address automatically** - Receives the DNS server address from a DHCP server.
- **Use the following DNS server addresses** - Allows you to add the DNS server's IP address(es) by hand.

**Figure 24-9 Internet Protocol Version 4 (TCP/IPv4) Properties**


Internet Protocol Version 4 (TCP/IPv4) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

**9** Click **OK** to close the **Internet Protocol Version 4 (TCP/IPv4) Properties** pop-up menu. Click **OK** again to close the **Local Area Connection Properties** pop-up menu.

**10** Attempt again to communicate to the network from your Client PC (For example, open your internet browser to see if you can reach a website). If you still cannot access the network, refer to Troubleshooting Network Connections on page 252.

**- End -**

# Troubleshooting Network Connections

If you have configured your entire NVR system but do not receive a response from one or more devices, you can use some basic network tools to evaluate your connectivity problems.

There are several commands that you can use from the Windows command prompt to help troubleshoot a network. From the DOS command prompt, you can use the following commands:

**1** **ipconfig /all** - This command displays the current settings on the client PC's NICs. These settings determine how the PC is connected to the network.

**2** **ping** -This command helps you determine if you can communicate with another computer in the network.

**3** **tracert** - This command displays where network data goes when it travels to a destination. It can help you find out where a network problem is located.

# Launching the Windows Command Prompt

To use the troubleshooting commands, we will need the Windows command prompt. To launch the command prompt, perform the following steps.

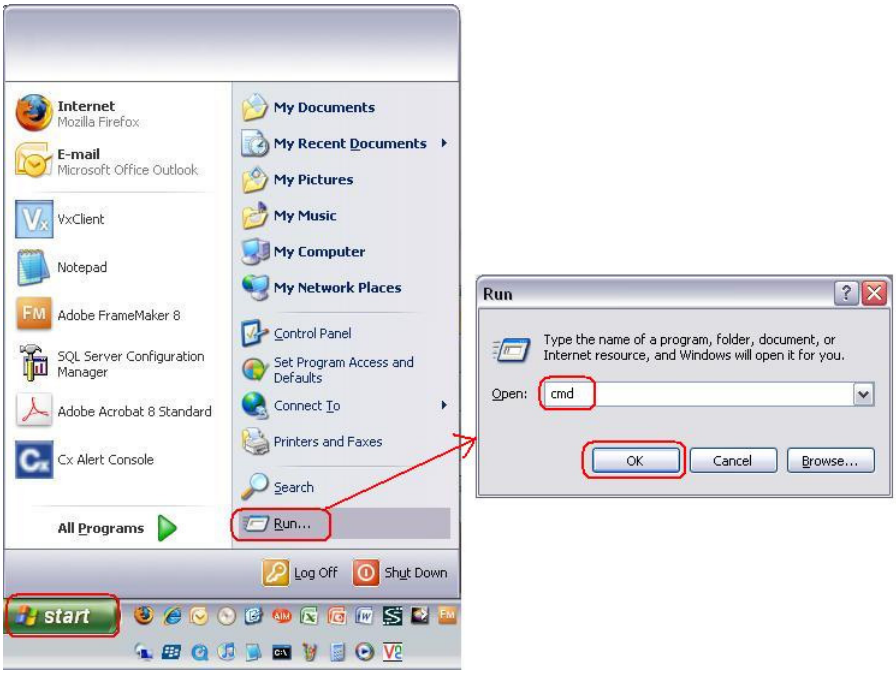
## Procedure 24-3
## Launch Windows Command Prompt (Windows XP)

| Step | Action |
|---|---|

1 Click **Start**, then **Run** in the Windows taskbar.

2 Type **cmd** in the field provided, then click **OK**.

**Figure 24-10 Start Then Run Commands.**




3 After clicking **OK**.

The command prompt window opens.

### Figure 24-11 Windows Command Prompt

## Procedure 24-4
## Launch the Windows Command Prompt (Windows 7)

| Step | Action |
|---|---|
| 1 | Click **Start** in the Windows taskbar. |
| 2 | Type **cmd** in the Search Programs and Files Field.<br>The Command Prompt Icon displays under the heading **Programs**. |
| 3 | Double-click the **Command Prompt Icon**.<br>The command prompt window opens. |

**Figure 24-12 Search for Command Prompt.**

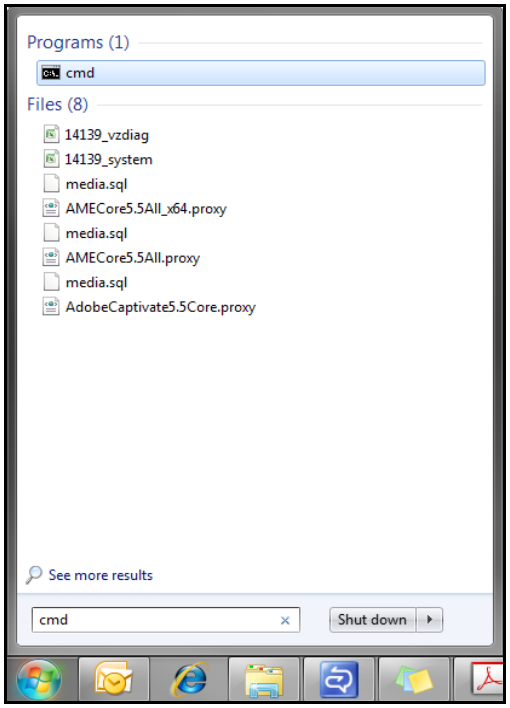
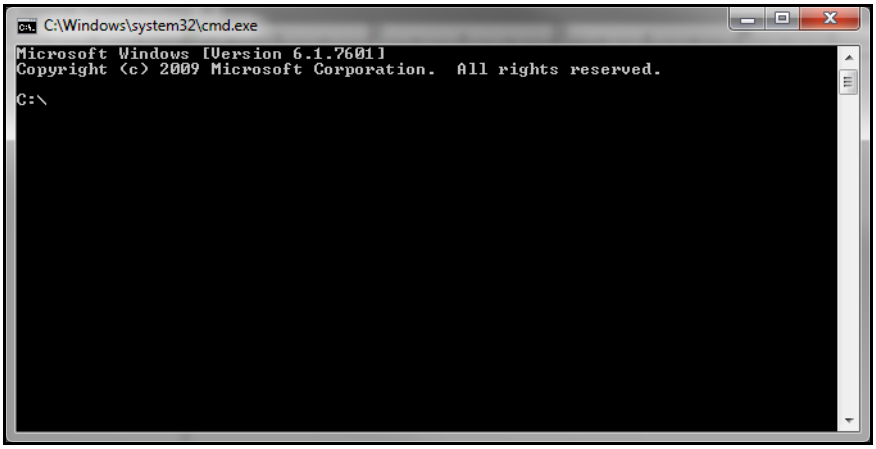



**Figure 24-13 Windows Command Prompt**




**- End -**

# Troubleshooting with the Ipconfig /All Command

The ipconfig /all command allows you to see all of the IP addresses that are used by your client PC. You will need this command to determine the IP addresses used by your NICs. The NIC connects your client PC to a TCP/IP network.

## Procedure 24-5
## Use the Ipconfig /All Command

| Step | Action |
|---|---|

**1** Open a Windows Command Prompt.

Refer to Procedure 24-3 Launch Windows Command Prompt (Windows XP)

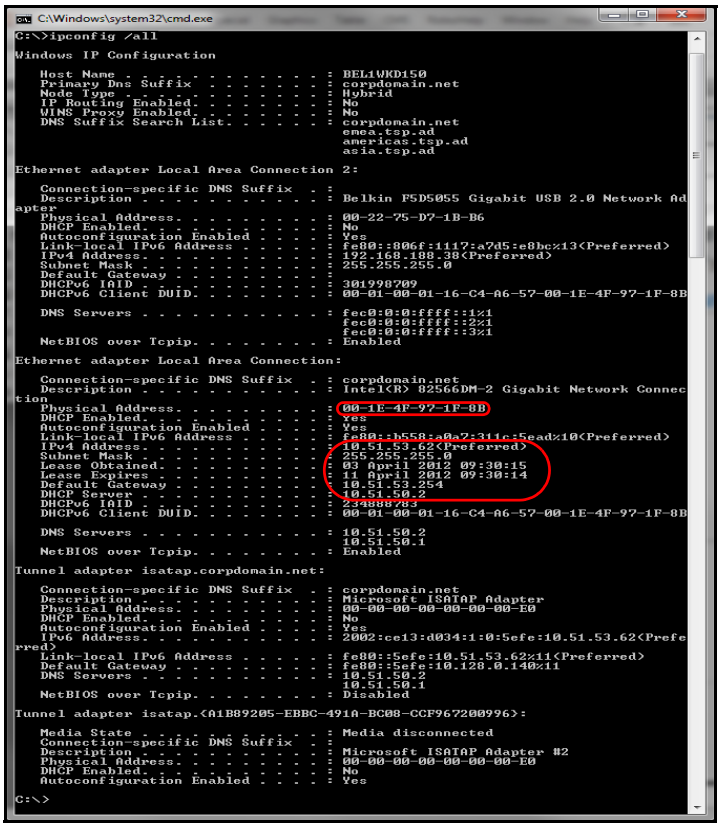
Or

Procedure 24-4 Launch the Windows Command Prompt (Windows 7).

**2** Type **ipconfig /all** in the Command Prompt window followed by the [Enter] key.

The configuration settings for all of your connections will display (Figure 24-14).

### Figure 24-14 IPCONFIG /ALL Command


C:\Windows\system32\cmd.exe
C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . : BEL1WKD150
Primary Dns Suffix . . . . . : corpdomain.net
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : corpdomain.net
emea.tsp.ad
americas.tsp.ad
asia.tsp.ad
Ethernet adapter Local Area Connection 2:
Connection-specific DNS Suffix . :
Description . . . . . : Belkin F5D5055 Gigabit USB 2.0 Network Adapter
Physical Address. . . . . : 00-22-75-D7-1B-B6
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::806f:1117:a7d5:e8bc%13(Preferred)
IPv4 Address. . . . . : 192.168.188.38(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . :
DHCPv6 IAID . . . . . : 301998709
DHCPv6 Client DUID. . . . . : 00-01-00-01-16-C4-A6-57-00-1E-4F-97-1F-8B
DNS Servers . . . . . : fec0:0:0:ffff::1%1
fec0:0:0:ffff::2%1
fec0:0:0:ffff::3%1
NetBIOS over Tcpip. . . . . : Enabled
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : corpdomain.net
Description . . . . . : Intel(R) 82566DM-2 Gigabit Network Connection
Physical Address. . . . . : 00-1E-4F-97-1F-8B
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::b558:a0a2:311c:5ead%10(Preferred)
IPv4 Address. . . . . : 10.51.53.62(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 03 April 2012 09:30:15
Lease Expires . . . . . : 11 April 2012 09:30:14
Default Gateway . . . . . : 10.51.53.254
DHCP Server . . . . . : 10.51.50.2
DHCPv6 IAID . . . . . : 234888703
DHCPv6 Client DUID. . . . . : 00-01-00-01-16-C4-A6-57-00-1E-4F-97-1F-8B
DNS Servers . . . . . : 10.51.50.2
10.51.50.1
NetBIOS over Tcpip. . . . . : Enabled
Tunnel adapter isatap.corpdomain.net:
Connection-specific DNS Suffix . : corpdomain.net
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv6 Address. . . . . : 2002:ce13:d034:1:0:5efe:10.51.53.62(Preferred)
Link-local IPv6 Address . . . . . : fe80::5efe:10.51.53.62%11(Preferred)
Default Gateway . . . . . : fe80::5efe:10.128.0.140%11
DNS Servers . . . . . : 10.51.50.2
10.51.50.1
NetBIOS over Tcpip. . . . . : Disabled
Tunnel adapter isatap.{A1B89205-EBBC-491A-BC08-CCF967200996}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
Description . . . . . : Microsoft ISATAP Adapter #2
Physical Address. . . . . : 00-00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
C:\>

**3** Verify the IP address(es) assigned tot he Client PC's Local Area Connection are correct (matches what you assigned, if you have assigned a static IP address).

**4** If any of the Default Gateway, DHCP Server, or DNS Server addresses are 0.0.0.0, it is likely that your Client PC is not communicating with the network correctly. Contact your network administrator for more information.

**- End -**

# Troubleshooting with the Ping Command

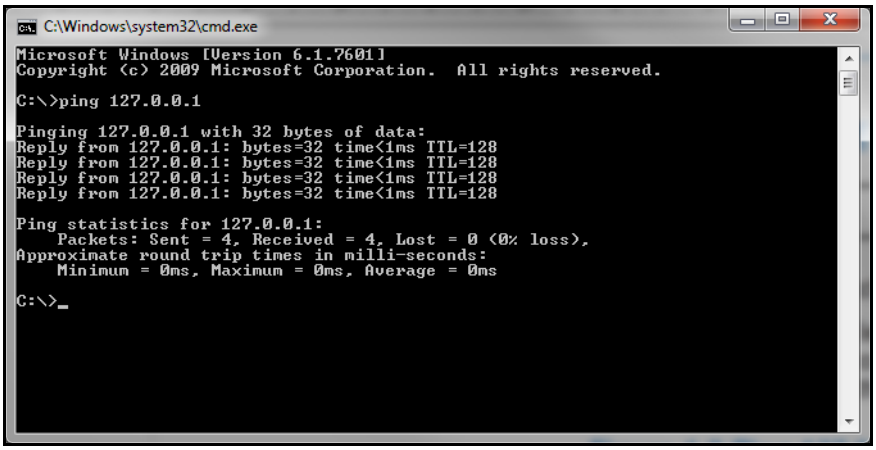
One of the most commonly used tools is the **ping** command. You can use the **ping** command to check the operation of:

- Client PC Local Ethernet Connection
- Client PC assigned IP address
- IP address and your connectivity to the NVR.

## Procedure 24-6
## Use of the Ping Command

| Step | Action |
|---|---|
| 1 | Open a Windows Command Prompt.<br>Refer to Procedure 24-3 Launch Windows Command Prompt (Windows XP)<br>Or<br>Procedure 24-4 Launch the Windows Command Prompt (Windows 7). |
| 2 | To determine if the Local Area Connection - Client PC NICs - is working properly, type **ping 127.0.0.1**. You should see the message “Reply from...” for a successful ping, or “Request has times out” if the ping was unsuccessful. |

**Figure 24-15 Ping 127.0.0.1**




| | |
|---|---|
| 3 | PING the IP address of your Client PC to verify it. For example, if the IP address is 192.168.0.100, type **ping 192.168.0.100**. If PING is unsuccessful (“Request timed out”), verify your configured IP address settings. |

4 PING the IP address of the NVR. If PING is unsuccessful (“Request timed out”), verify the IP address of the NVR.

**Note**

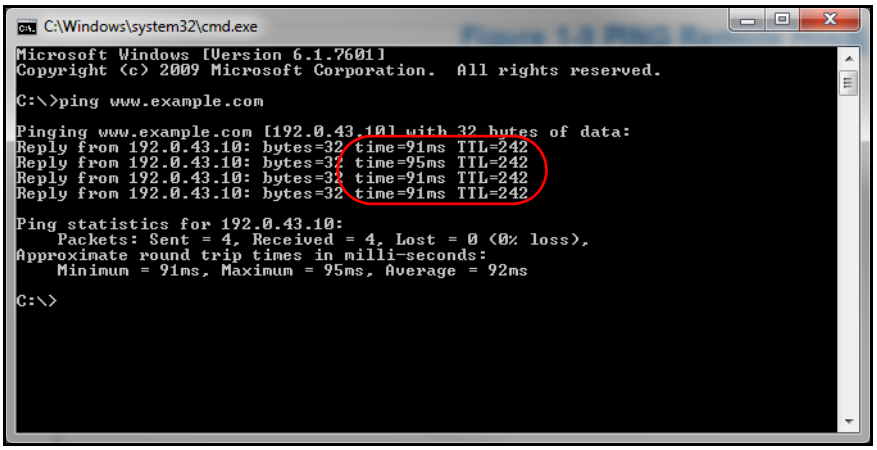
The default IP address for eth0 of the NVR when supplied as a hardware and software bundle is 10.10.10.10, all other NICs will be disabled.
It is likely that the NVR has been re-assigned a new IP address that is in the same network as your Client PC. If neither the assigned IP address for the NVR nor the default IP address of the NVR can be successfully pinged, your Client PC or the NVR (or both) are experiencing connectivity problems. You should contact your network administrator.

5 When using the PING command, it also displays how long the packet took to reach its destination. This comes in very handy when checking for network latency.

**Note**

If the delay is too long, it may indicate that your attempts to connect to the NVR are timing out, even if PING does not time out. Contact your network administrator to determine the source of the network delay.

**Figure 24-16 PING Remote Host**


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>ping www.example.com
Pinging www.example.com [192.0.43.10] with 32 bytes of data:
Reply from 192.0.43.10: bytes=32 time=91ms TTL=242
Reply from 192.0.43.10: bytes=32 time=95ms TTL=242
Reply from 192.0.43.10: bytes=32 time=91ms TTL=242
Reply from 192.0.43.10: bytes=32 time=91ms TTL=242
Ping statistics for 192.0.43.10:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 91ms, Maximum = 95ms, Average = 92ms
C:\>

**- End -**

# Troubleshooting with the Tracert Command

Another tool that can be used is the **Tracert** command. This command will display other network devices that are along the path from which the packet took to reach its destination. This tool is best for locating a single point of failure on a network.

## Procedure 24-7
## Use of the Tracert Command

| Step | Action |
|---|---|

**1** Open a Windows Command Prompt.

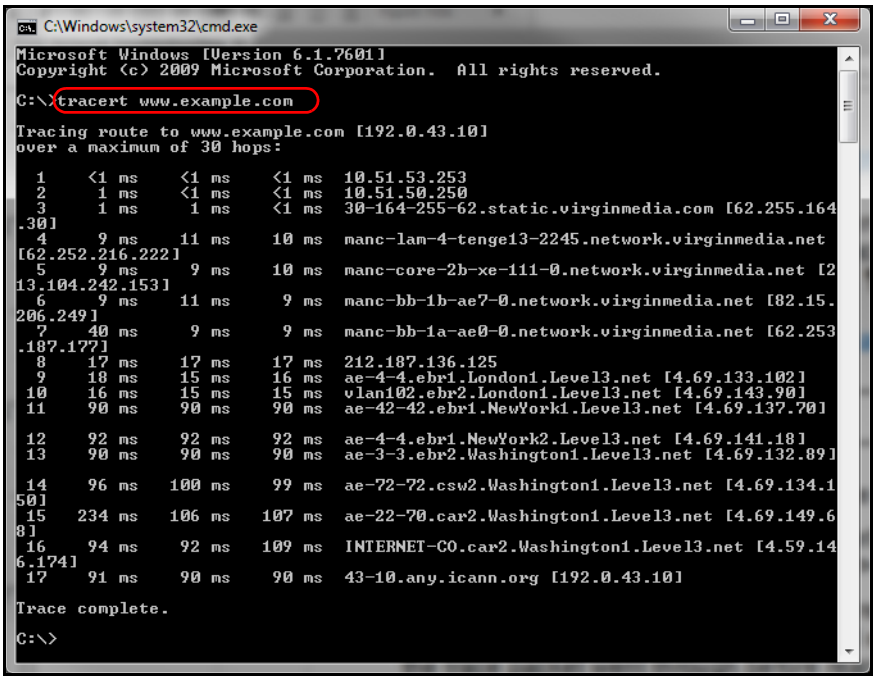
Refer to Procedure 24-3 Launch Windows Command Prompt (Windows XP)

Or

Procedure 24-4 Launch the Windows Command Prompt (Windows 7).

**2** To use **tracert** to trace the connection between your Client PC and the NVR, type **tracert <IP address of the NVR>**.
The **tracert** function will displays in the command prompt window. A typical **tracert** output is shown in Figure 24-17(in this case, an example of a **tracert** to *www.example.com*. You can see several entries of different switches and/or routers that the trace packet went through before reaching its destination:

**Figure 24-17 Using the Tracert Command**


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\>tracert www.example.com
Tracing route to www.example.com [192.0.43.10]
over a maximum of 30 hops:
1 <1 ms <1 ms <1 ms 10.51.53.253
2 1 ms <1 ms <1 ms 10.51.50.250
3 1 ms 1 ms <1 ms 30-164-255-62.static.virginmedia.com [62.255.164.30]
4 9 ms 11 ms 10 ms manc-lam-4-tenge13-2245.network.virginmedia.net [62.252.216.222]
5 9 ms 9 ms 10 ms manc-core-2b-xe-111-0.network.virginmedia.net [213.104.242.153]
6 9 ms 11 ms 9 ms manc-bb-1b-ae7-0.network.virginmedia.net [82.15.206.249]
7 40 ms 9 ms 9 ms manc-bb-1a-ae0-0.network.virginmedia.net [62.253.187.177]
8 17 ms 17 ms 17 ms 212.187.136.125
9 18 ms 15 ms 16 ms ae-4-4.ebr1.London1.Level3.net [4.69.133.102]
10 16 ms 15 ms 15 ms vlan102.ebr2.London1.Level3.net [4.69.143.90]
11 90 ms 90 ms 90 ms ae-42-42.ebr1.NewYork1.Level3.net [4.69.137.70]
12 92 ms 92 ms 92 ms ae-4-4.ebr1.NewYork2.Level3.net [4.69.141.18]
13 90 ms 90 ms 90 ms ae-3-3.ebr2.Washington1.Level3.net [4.69.132.89]
14 96 ms 100 ms 99 ms ae-72-72.csw2.Washington1.Level3.net [4.69.134.150]
15 234 ms 106 ms 107 ms ae-22-70.car2.Washington1.Level3.net [4.69.149.68]
16 94 ms 92 ms 109 ms INTERNET-CO.car2.Washington1.Level3.net [4.59.146.174]
17 91 ms 90 ms 90 ms 43-10.any.icann.org [192.0.43.10]
Trace complete.
C:\>

**3** If you see “* * * Request timed out.”, it means that tracert was unable to contact the NVR at the address you typed. You should contact your network administrator to confirm the IP address for the NVR.

**4** If the tracert is unable to contact the network for the NVR IP address (for example, the trace request times out at 192.168.200.4 when you typed an address of 192.168.10.45), then the problem might be with a network device other than the NVR. You can show the tracert result to your network administrator to help diagnose the problem.

**Note**

If you are still experiencing connectivity issues, then there are some other items you can troubleshoot:

- Hardware Connectivity.
- Software Configuration.
- Anything associated with the network devices you are working with.

**- End -**

# Appendix D: NVR Troubleshooting

## Overview

The NVR has an embedded Linux-based operating system (SUSE) which is used during the setup and installation process for the initial configuration of the NVR's network settings. The NVR desktop can be used to re-enable network access should the NVR become unaccessible when enabling/disabling NICs using the NVR Web Interface. The NVR desktop can also be used to edit system settings or configure storage partitions.

Alternatively a Remote Desktop Connection can also be established allowing you to edit the network settings using the NVR desktop from a remote client.

## Enabling Remote Desktop

The NVR's desktop can be accessed from a remote PC using either Remote Desktop Protocol or Video Network Computing.

### Enabling RDP Remote Desktop

Remote Desktop Protocol is a proprietary protocol developed by Microsoft. It allows you to access the NVR's desktop from a remote PC using the Remote Desktop Connection application.

Remote Desktop Connection may affect the performance of your NVR if it is fully configured. If you are concerned by possible effects on performance you should use the VNC method of establishing a remote desktop instead.

**Note**

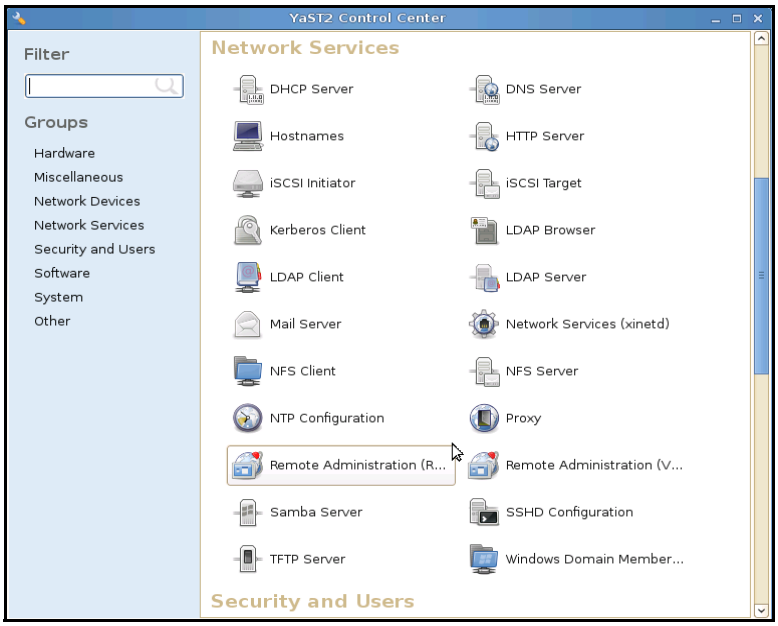
Connection is usually through port 3389.

#### Procedure 25-1
#### Enabling RDP Remote Desktop

| Step | Action |
|---|---|
| 1 | Click **Computer**. |
| 2 | Select **YaST**. |

The Control Center opens.

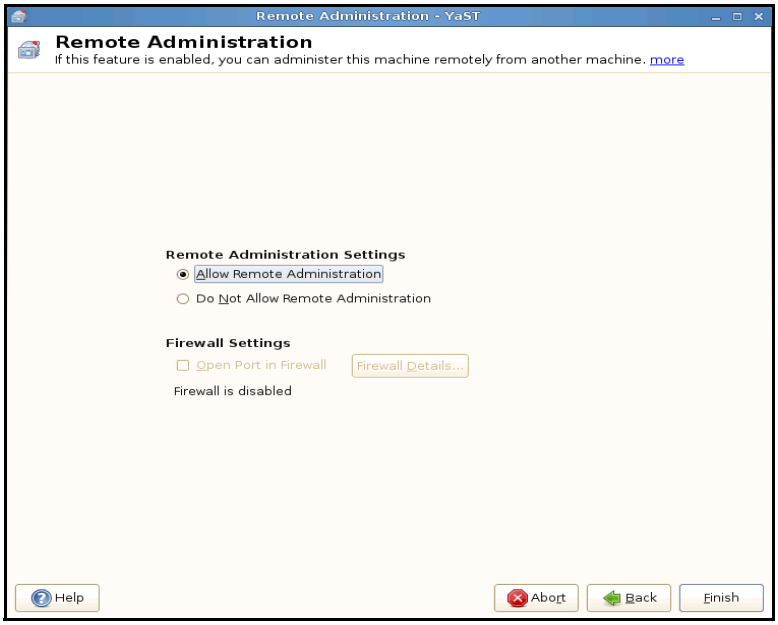
**Figure 25-1 Control Center**




3 Click **Remote Administration (RDP)**. Refer to Figure 25-3 Control Center.

The Remote Administration window opens.

**Figure 25-2 Remote Administration**




4 Select **Allow Remote Administration**. Refer to Figure 25-4 Remote Administration.

5 Click **Finish**.

**- End -**

# Enabling VNC Remote Desktop

Virtual Network Computing (VNC) settings can be enabled which will allow you to access the NVR's desktop from a remote PC using your web browser and Java. VNC is platform-independent so more than one user can access the NVR's desktop at once.

**Note**

Connection is usually through port 5801.

## Procedure 25-2
## Enabling and Disabling Remote Desktop Settings

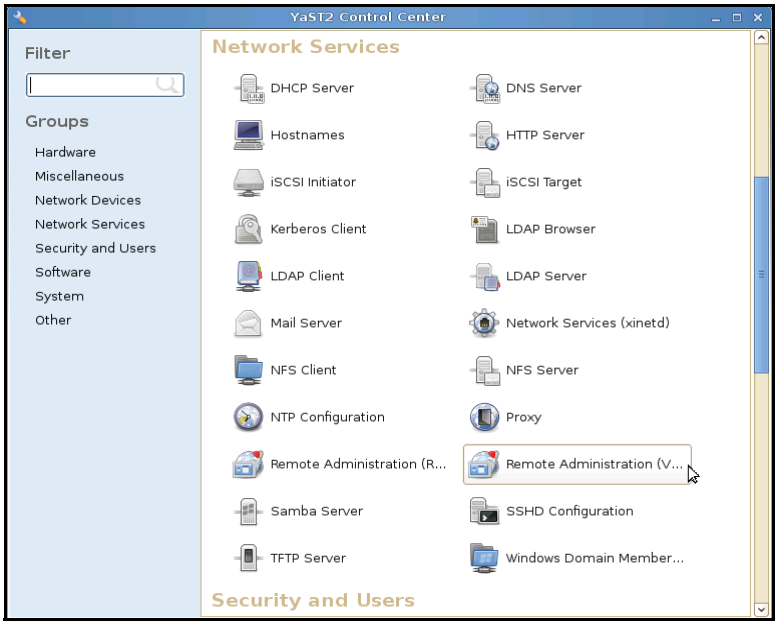
| Step | Action |
|---|---|

1 Click **Computer**.

2 Select **YaST**.

The Control Center opens.

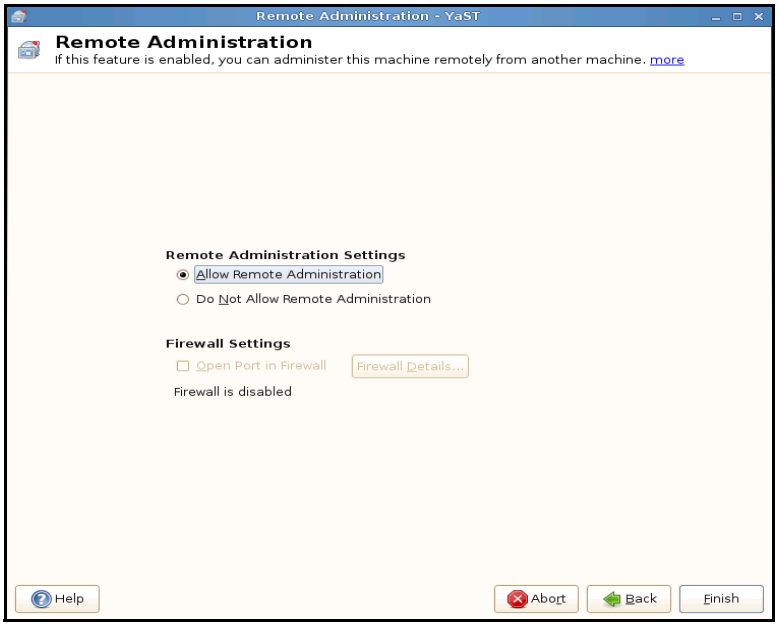
**Figure 25-3 Control Center**




3 Click **Remote Administration (VNC)**. Refer to Figure 25-3 Control Center.

The Remote Administration window opens.

**Figure 25-4 Remote Administration**




4 Select **Allow Remote Administration**. Refer to Figure 25-4 Remote Administration.

5 Click **Finish**.

**- End -**

# Accessing the Remote Desktop

## RDP Remote Desktop

The following procedures will allow you to log on and log off RDP remote desktop.

### Procedure 25-3
### Logging in to RDP Remote Desktop

| Step | Action |
|---|---|

1 Click **Start** in the Windows taskbar.

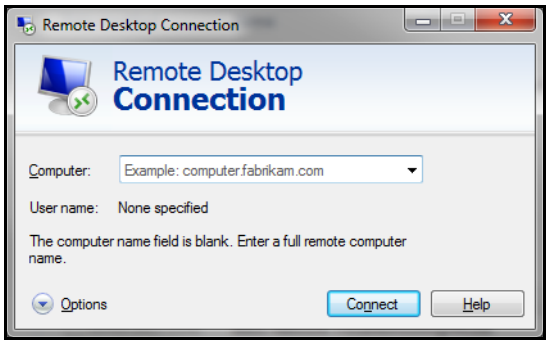
2 Select **All Programs**.

3 Select **Accessories**.

4 Select **Remote Desktop Connection**.

The Remote Desktop Connection application opens.

**Figure 25-5 Remote Desktop Connection**




5 Enter the **NVR's IP Address** in the Computer field.

6 Select **Options**.

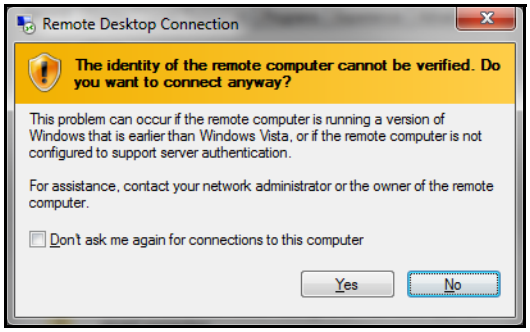
The application expands.

7 Select **Display**.

8 From the Colors dropdown select **High Colour (16 bit)**.

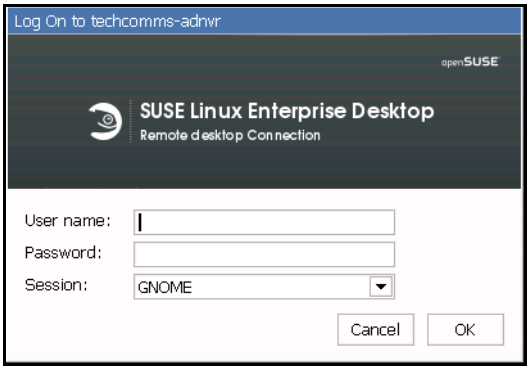
9 Click **Connect**.

A warning displays.


Remote Desktop Connection
The identity of the remote computer cannot be verified. Do you want to connect anyway?
This problem can occur if the remote computer is running a version of Windows that is earlier than Windows Vista, or if the remote computer is not configured to support server authentication.
For assistance, contact your network administrator or the owner of the remote computer.
Don't ask me again for connections to this computer
Yes
No

10 Click **Yes**.

The NVR's Desktop Login window opens.

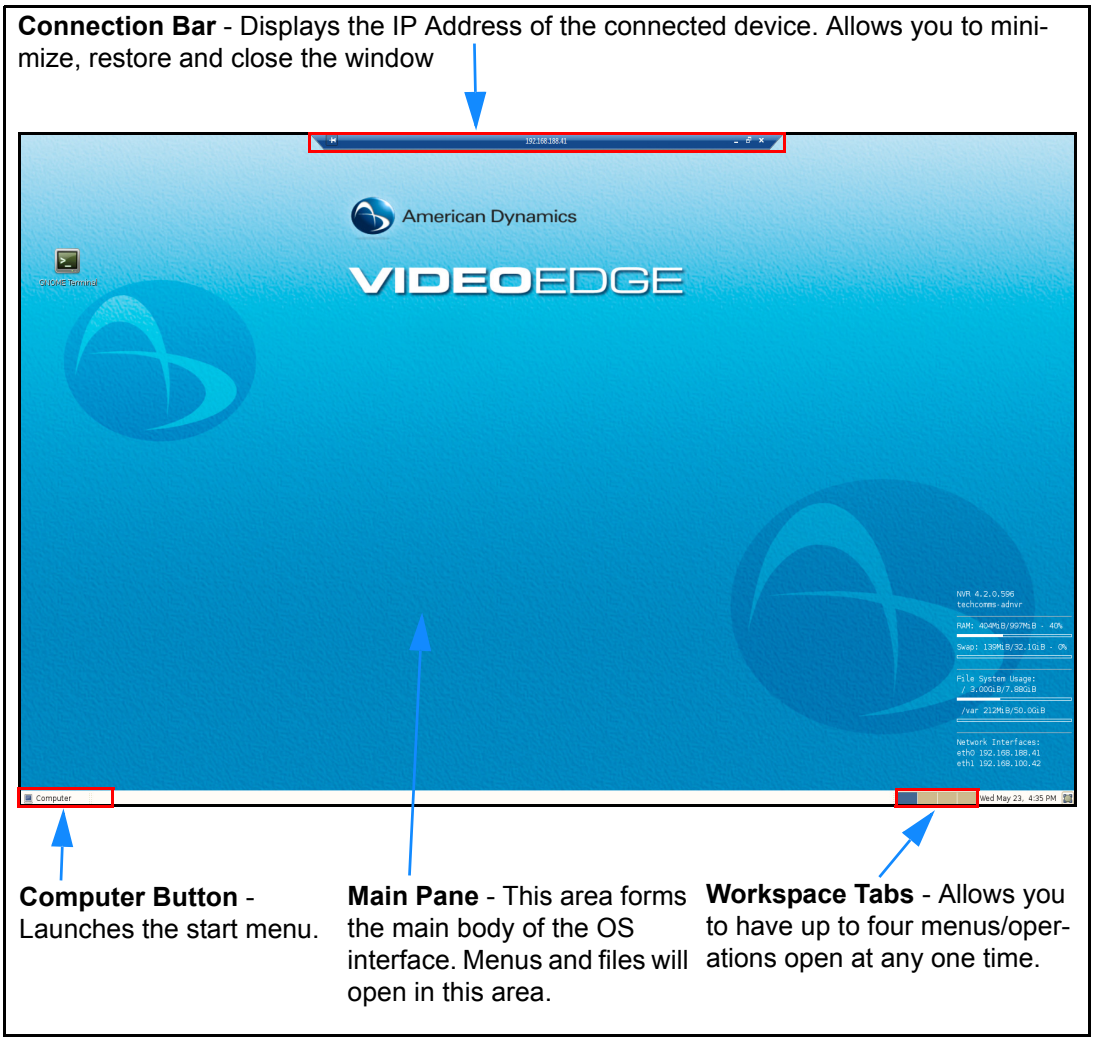



11 Enter the **username** and **password** in the corresponding fields.

12 Click **OK**.

**- End -**

**Figure 25-6 NVR Remote Desktop Interface (RDP)**


**Connection Bar** - Displays the IP Address of the connected device. Allows you to minimize, restore and close the window
American Dynamics
VIDEOEDGE
Computer
**Computer Button** - Launches the start menu.
**Main Pane** - This area forms the main body of the OS interface. Menus and files will open in this area.
**Workspace Tabs** - Allows you to have up to four menus/operations open at any one time.

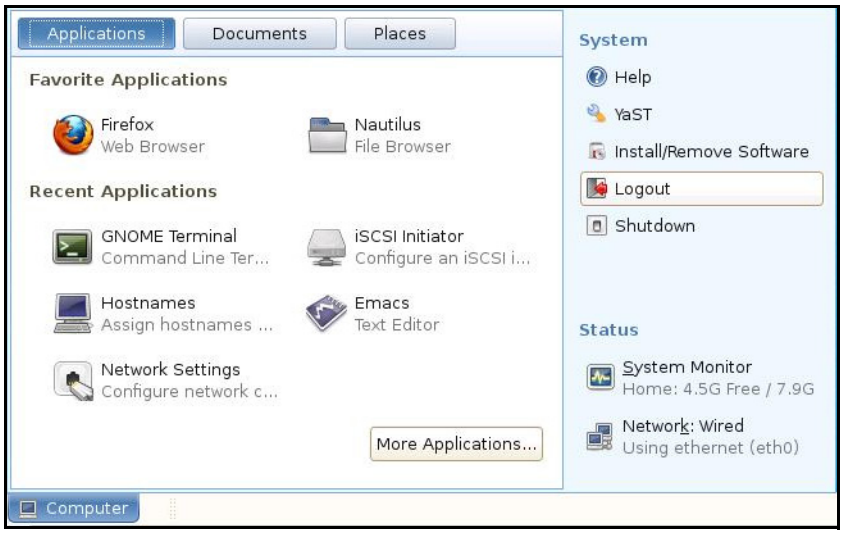
## Logging Out of RDP Remote Desktop

When using RDP remote desktop it is important to logout correctly. Failure to do so will leave a high CPU process running on the NVR which will affect performance.

### Procedure 25-4
### Logging Out of RDP Remote Desktop

| Step | Action |
|---|---|
| 1 | Click **Computer**. |
| 2 | Select **Logout**. |
| | A popup window opens. |

**Figure 25-7 Logout Icon**




**3** Select **Log Out**.

Remote Desktop window closes.

**Figure 25-8 Logout Popup**

Log Out of the Session
Log Out
Ends your session and logs you out.
Switch User
Suspends your session, allowing another user to log in and use the computer.
You are currently logged in as "root".
You will be automatically logged out in 60 seconds.
Help
Cancel

**4** Select to close the Remote Desktop Connection application.

**- End -**

## VNC Remote Desktop

The following procedures will allow you to log on and log off VNC remote desktop.

## Procedure 25-5
## Logging in to VNC Remote Desktop

| Step | Action |
|---|---|

**1** Launch your web browser and enter the NVR's IP address into the URL field followed by **:5801**. For example, if your NVR's IP address was 100.100.100.100, enter the address as below:

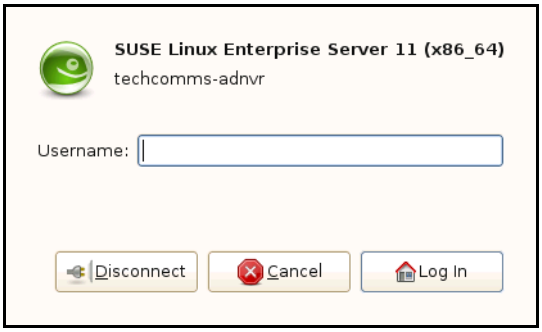
**Note**

To use the remote desktop function your browser must be Java enabled, access is achieved through the TCP port 5801.

**2** Press **[Enter]**.

The Remote Desktop page opens.

**Figure 25-9 NVR Desktop Login Window (VNC)**




**3** Enter your **Username**.

**Note**

If you are planning to change system settings, you need to login as the System Administrator (**root**).

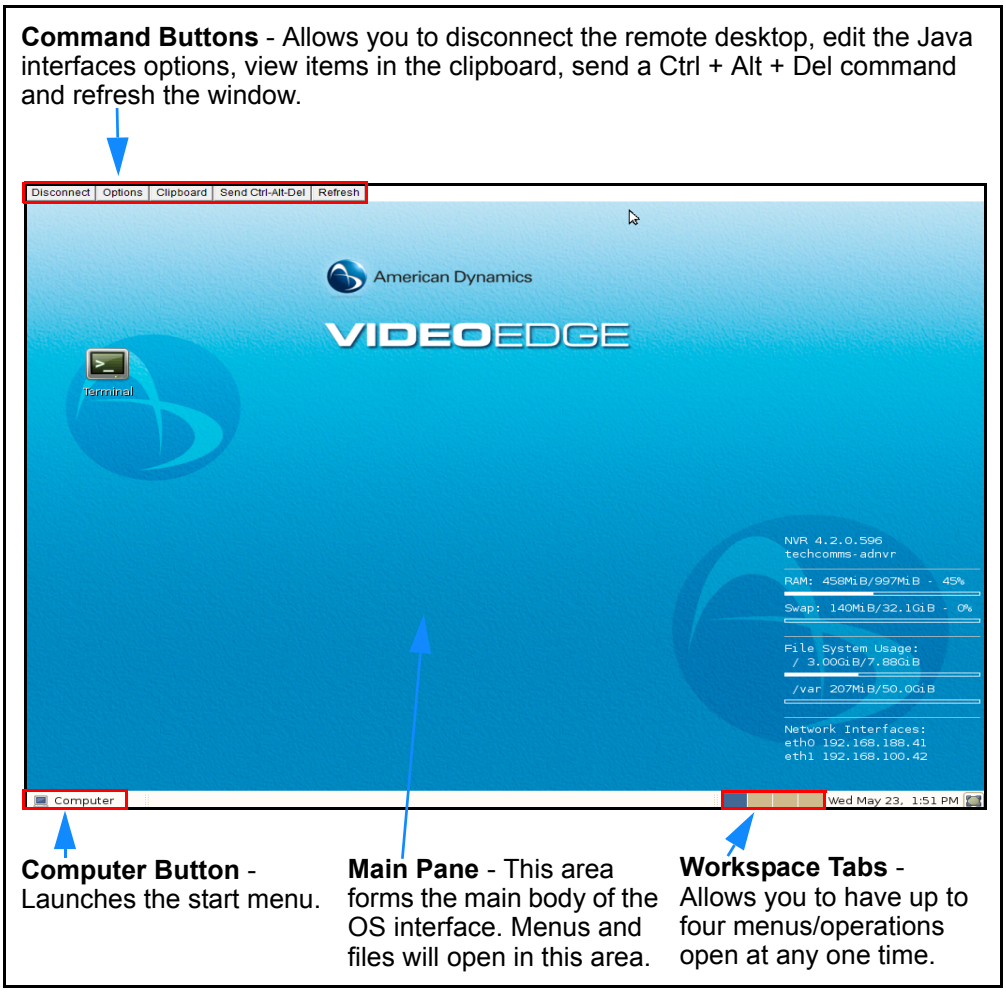
**4** Click **Log In**.

**5** Enter your **Password**.

**6** Click **Log In**.

**- End -**

## Figure 25-10 NVR Remote Desktop Interface (VNC)


**Command Buttons** - Allows you to disconnect the remote desktop, edit the Java interfaces options, view items in the clipboard, send a Ctrl + Alt + Del command and refresh the window.
Disconnect
Options
Clipboard
Send Ctrl-Alt-Del
Refresh
American Dynamics
VIDEOEDGE
Terminal
NVR 4.2.0.596
techcomms-adnvr
RAM: 458MiB/997MiB - 45%
Swap: 140MiB/32.1GiB - 0%
File System Usage:
/ 3.00GiB/7.88GiB
/var 207MiB/50.0GiB
Network Interfaces:
eth0 192.168.188.41
eth1 192.168.100.42
Computer
Wed May 23, 1:51 PM
**Computer Button** - Launches the start menu.
**Main Pane** - This area forms the main body of the OS interface. Menus and files will open in this area.
**Workspace Tabs** - Allows you to have up to four menus/operations open at any one time.

## Procedure 25-6
## Logging Off VNC Remote Desktop

| Step | Action |
|---|---|
| 1 | Click the **Disconnect** command button.<br>VNC Remote Desktop is disconnected. |

**- End -**

## Editing the Network Settings Using Control Center

You can edit the NVR's network settings using the Control Center tool within the NVR desktop.

**Note**

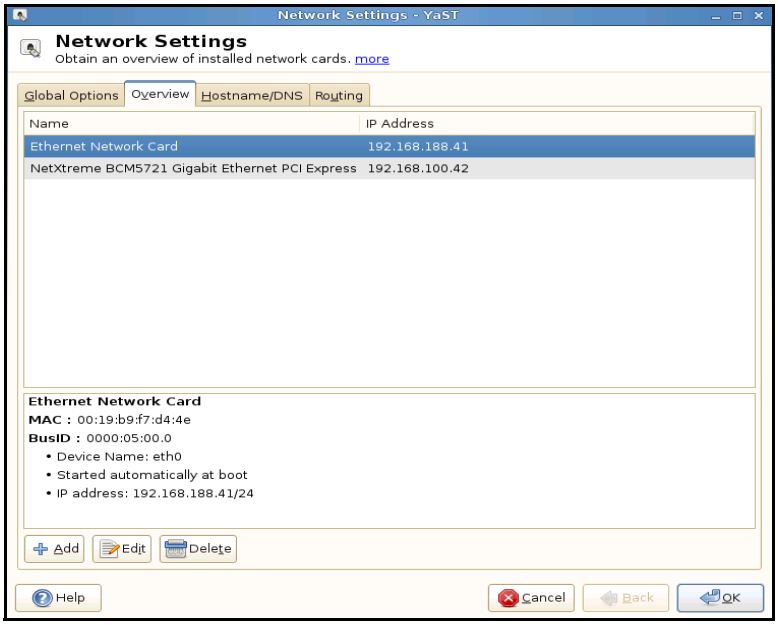
To make changes to the NVR system using the Control Center you must ensure you are logged in as the Root user.

### Procedure 25-7
### Editing the NVR's Network Settings Using Control Center

| Step | Action |
|---|---|
| 1 | Log in to the NVR desktop locally or using a remote desktop connection, refer to Procedure 25-5 Logging in to VNC Remote Desktop on page 268. |
| 2 | Click **Computer**. |
| 3 | Select **YaST**.<br>The Control Center opens. |
| 4 | Click **Network Settings**. Refer to<br>The Network Settings window opens. |

**Figure 25-11 Network Settings Icon**

**Figure 25-12 Network Settings Window**




5 Select the **NIC** you want to edit.

6 Click **Edit**.

**Note**

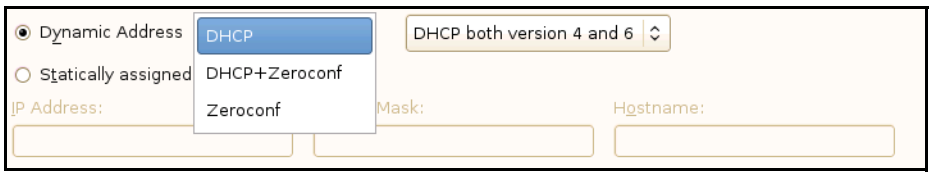
The available options for editing are sorted under three tabs, General, Address and Hardware. These tabs provide several more options than the NVR Web Interface, for more information on the options provided by the General and Hardware tab you should contact your Network Administrator.

7 Select the **Address** tab.

8 Select **Dynamic Address**.

**a** From the dropdown select either **DHCP**, **DHCP + Zeroconf** (Zero Configuration Networking) or **Zeroconf**.

**b** From the dropdown select either **DHCP both version 4 and 6**, **DHCP version 4 only** or **DHCP version 6 only**.



Or

Select **Statically assigned IP Address.**

**a** Enter the **IP address** in the IP Address field.

**b** Enter the **Subnet Mask** in the Subnet Mask field.

**c** Enter the **Hostname** in the Hostname field.

**9** Click **Next**.

**10** To edit another NIC repeat steps 5-9.

**11** Click **OK**.

**- End -**

# Editing Storage Partitions Using Partitioner

## Configuring System Partitions on a Previously Configured Device

If you are installing or upgrading the NVR software on a device which has been previously configured, there may be system partitions created already which will require re-configuration. To ensure your NVR is set up correctly, the existing system partitions should be deleted.

The requirements for configuration are three system partitions in addition to the media storage partitions. The system partitions are needed for regular operation of the NVR's operating system. The required system partitions that need to be created are outlined in Table 25-1. Each partition size in the table is the recommended minimum value.

**Table 25-1 Default Partitions Required for NVR**

| Size (GB) | Type | FS Type | Mount Point |
|---|---|---|---|
| 16 | Linux swap | Swap | swap |
| 476 | Linux native | XFS | /var |
| 8 | Linux native | Ext3 | / |

### Procedure 25-8
### Configuring System Partitions on a Previously Configured Device

**Step Action**

**1** In the Suggested Partioning page of the Partitioner Wizard, click **Create Partition Setup**.

**2** Select **Custom Partitioning (for experts)**.

The Expert Partitioner page displays.

3 To edit the partitions and create partitions for media storage **Select the disk** on which you want to create the media partition from the system view tree.

4 **Delete** the existing partitions, by selecting the partition and clicking **Delete**.

5 Click **Add.**

6 Select **Primary Partition**.

7 Enter the required partition size by selecting **Custom Size** and entering the amount of disk space (GB) you want to allocate to the partition.

Or

Choose an allocated region on the disk for the partition by entering a **Start Cylinder** and **End Cylinder**.

8 Select **Next**.

9 Select the desired option from the **File System** dropdown. For swap select **Swap**, for var select **XFS** and for root select **Ext3**.

Or

10 Enter the **Mount Point** for the media partition. For swap enter **swap**, for var enter **/var** and for root enter **/**.

11 Click **Finish**.

12 Create the required media storage partitions. Refer to Steps 5 to 11 of Procedure 3-8 Configuring Media Partitions on the Remaining Media Drives on the NVR on page 15 for further information.

13 Once all media partitions are created click **Accept**.

A summary of the partitions to be created are displayed. If you want to edit any of the partitions click **Edit Partition Setup** and make the changes as required.

14 Click **Next.**

A summary of the partition layout to be created is displayed.

15 Click **Install.**

The Confirm Installation page is displayed.

16 Click **Install**.

The NVR Installation begins.

**Note**

Installation can take up to ten minutes.

17 After basic installation is complete the system will need to be restarted. Continue to Procedure 3-10 Rebooting the NVR After Basic Installation on page 21.

**- End -**

# Editing Media Partition Configurations

If you have completed the installation of the NVR hardware and software bundle, default media partitions will be configured on the NVR. You can change these media partitions to suit your specific requirements.

If you want to edit media partition configurations on a storage device you must remove all media folders already configured to be used by the NVR from the NVR configuration. Refer to Disabling Storage Media Folders on page 62 for information.

**Note**

If a storage set contains only media folders from the device you want to edit media partition configurations on, you must move camera recording to other storage sets first. Refer to Advanced Storage Configuration on page 65 for further information.

NVR Services should also be stopped prior to changing partition configurations on devices that have already been added to the NVR. Refer to Procedure 16-2 Stop NVR Services on page 170 for further information.

## Procedure 25-9
## Editing Media Partitions

| Step | Action |
|---|---|

**1** Select **Computer** from the NVR desktop.

**2** Select **YaST** from the System menu.

The Control Center opens.

**3** Select **Partitioner** from the System menu.

**4** A warning message opens. Click **Yes** to continue.

The Expert Partitioner page opens.

**5** Select the disk containing the media partitions you want to edit from the system view tree.

**6** To edit the size of a partition:

- **a** Select the partition in the table and click **Resize**.
- **b** Select either **Maximum Size**, **Minimum Size** or **Custom Size** and enter the required partition size.
- **c** Click **OK**.

Or

To add a new partition:

- **a** Click **Add**.
- **b** Select either **Primary Partition** or **Extended Partition**.
- **c** Select the partition size. Select either **Maximum Size**, **Minimum Size** or **Custom Size** and enter the required partition size. If preferred you can choose an allocated region of the disk by entering a **Start Cylinder** and an **End Cylinder**.
- **d** Select **Next**.
- **e** If you are creating an extended partition, continue to step l otherwise continue to step f.
- **f** Click the **Format Partition** option button.
- **g** Select **XFS** from the **File System** dropdown.
- **h** Enter the **Mount Point** for the media partition, for example, **/data/media1**.
- **i** Select the **Fstab Options...** button.

j Enter **rw,noatime,nodiratime,attr2,nobarrier,noquota,allocsize=4m** in the **Arbitrary option value** field.

**Note**

**nobarrier** should only be used on storage devices connected to disk controllers with battery backed cache.

k Click **OK**.

l Click **Finish**.

Or

To delete a partition:

a Select the partition you want to delete.

b Click **Delete**.

c Click **Confirm** to delete the partition.

7 Click **Next.**

The Expert Partitioner page opens displaying the changes to be made to the partitions.

8 Click **Finish**.

The changes are made to the partitions.

**- End -**

# System Disk Recovery

## VideoEdge NVR

Should the NVR's system disk fail or the system disk becomes corrupt, the following procedure should be used for its recovery. You will need the following items:

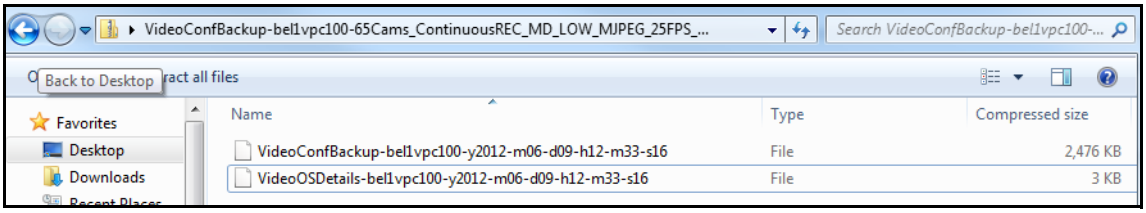
1 A Licence file for the NVR.

2 A system backup file (from **NVR 4.2+ only**).

**Note**

You must have carried out a "backup" procedure after all NVR configuration was completed at time of install (Procedure 3-30 Completing the NVR Setup on page 49 or Procedure 17-3 Creating a Configuration Backup File on page 181). This is a zip file which when expanded contains two files. One of the files is the NVR backup information (Named "VideoConfBackup-xxxxxxxxxxx.zip". The other is a text file detailing Network and storage mount information. This text file, VideoOSDetails-xxxxxxxx.zip, is required to complete the recovery procedure.

**Figure 25-13 Backup Information Files**




3 A replacement disk greater than the existing system disk (if applicable).

4 NVR 4.2.1 Software CD or USB drive.

## Procedure 25-10
## VideoEdge NVR System Disk Recovery

| Step | Action |
|---|---|

1 Power **OFF** the NVR.

2 (Optional) Replace the system disk. This step is required if the system disk becomes corrupt.

3 Ensure all external connections are present.

4 Boot the NVR from the 4.2.1 Software CD or USB drive.

5 Complete the Installation process as far as the VideoEdge Setup Wizard stage. Refer to Installing the NVR Software Only Bundle on page 10 for installation instructions.

6 Using YaST configure any iSCSI storage devices and connect to them. Refer to Procedure 22-3 Connecting NVR to FRS/FES Using iSCSI on page 230.

7 Unzip the backup file in windows. Extract the file "**VideoOSDetails-VideoEdge-XXXXXXXX**" and save to a USB.

8 On the NVR, open the file "**VideoOSDetails-VideoEdge-XXXXXXXX**" from the USB in a text editor.

9 Copy all information from the Filesystem details section of the file.

10 Paste the copied text into a new file, **/tmp/fstab_backup** on the NVR.

- **a** Open the Terminal window.
- **b** Type **cat>/tmp/fstab_backup**. Press **[Enter]**.
- **c** Paste the copied text from the clipboard. Press **[Enter]**.
- **d** Press **[CTRL] + [D]**.

11 In the Terminal window type **videoedge# /opt/americandynamics/venvr/bin/restore_fstab/tmp/fstab_backup** and press **[Enter]**.

Running this command restores all previous mountpoints.

12 On the NVR desktop double-click on the **NVR Administrator** icon, or on a remote machine use Internet Explorer to log into the NVR Configuration Interface. The default credentials are Username: **admin**, Password: **VIDEO!edge23**.

The Setup Wizard opens at the Welcome page.

13 Click **Start** to begin the Setup Wizard.

The first step is to apply your licence. Apply the NVR 4.2.1 licence file and click **Continue**. For further information on how to apply a license, refer to Procedure 3-14 Configuring the

Setup Page on page 28.

**14** Continue through the Setup Wizard until you reach the Network section of the wizard. Open the “VideoOSDetails-xxxxxxxx” file and use the network settings to help you configure the following:

- Domain Name
- Domain Name Servers
- Default Gateway
- RTSP Port
- NTP Status
- NTP Servers
- Network Interfaces
- DHCP Configuration

**15** Complete the remaining stages of the Setup Wizard.

When complete the NVR Configuration Interface opens at the Camera List page.

**16** Select **System**.

**17** Select **Backup/Restore**.

The Backup page opens.

**18** Select the **Restore** tab.

The Restore page opens.

**19** Click **Browse**.

**20** Navigate to and select the NVR backup file, “**VideoConfBackup-xxxxxxxxxxx.zip**”.

**Note**

You must use the zip file and not an individual sub file.

**21** Click **Upload Backup**.

**22** You will be prompted for media recovery, click **Yes**. Media recovery will take approximately 1 minute per 90-100GB of Storage.

Status messages will display informing you of current progress.

**23** Once complete verify that all configuration parameters are correct.

**- End -**

# Appendix E: Upgrading your NVR 4.1

## Overview

The NVR 4.2.1 software includes an upgrade package for users currently using the NVR 4.1 software. The upgrade process is mainly automated, information and instructions are provided as the process runs within Linux Terminal.

The upgrade process preserves the following of your NVR's files and settings:

- Media Database
- Camera Settings
- Alarm Settings
- Storage Settings
- Network Settings

The installation consists of three stages:

**1** Backup NVR 4.1 applications and OS settings.

**2** Installation of NVR 4.2.1 software.

**3** Restoration of NVR 4.1 application and OS settings.

Should the upgrade fail an error code will be presented to you with details of the log file location. This should be supplied to American Dynamics support.

After a successful upgrade you should create a backup file of your NVR 4.2.1. This can be used to retain your current system settings if you need to perform a system disk recovery in the future.

### Download and Deletion of NVR 4.1 ISO Files

ISO data will be preserved during the upgrade process and will consume storage space for future recording. It is recommended prior to beginning the upgrade process that you download and delete all ISO data from the NVR 4.1.

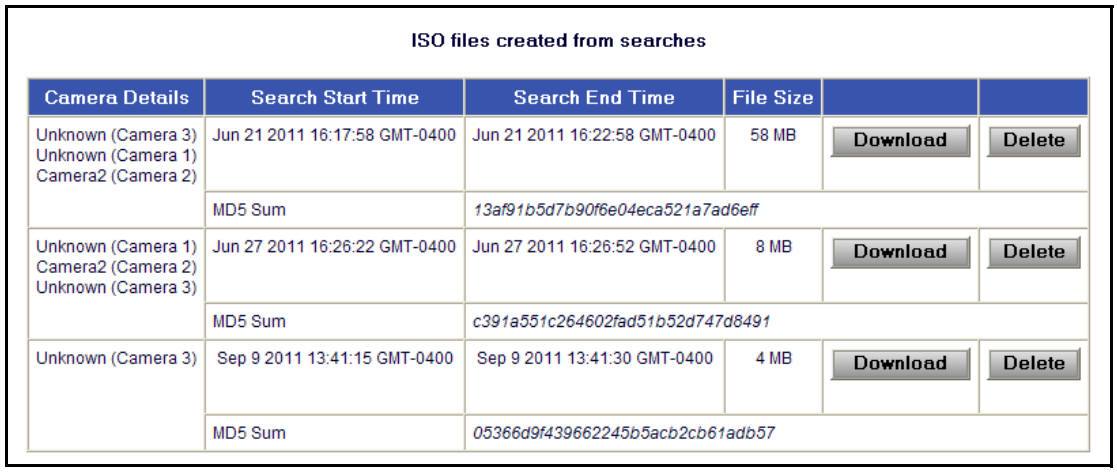
#### Procedure 26-1
#### Downloading NVR 4.1 ISO Files

| Step | Action |
|---|---|
| **1** | Select **Video**. |

2 Select **ISO Files**.

3 Each ISO file is listed with its relevant data.

**Figure 26-1 ISO Files**




4 Click **Download**, a Windows Save dialog opens so that you can save an ISO file to an available file path.

**- End -**

### Procedure 26-2
### Deleting NVR 4.1 ISO Files

| Step | Action |
|---|---|

1 Select **Video**.

2 Select **ISO Files**.

3 Each ISO file is listed with its relevant data.

4 Click **Delete**, the selected ISO file(s) are deleted.

**- End -**

# NVR 4.1 to NVR 4.2.1 Upgrade

To initialize the upgrade of the NVR, the system must boot from the software disk/USB.

## Procedure 26-3
## Launching the Upgrade Tool

| Step | Action |
|---|---|
| 1 | Insert the NVR software CD into the CD/DVD drive or insert the NVR Installation USB drive into a USB port. |
| 2 | Take screen shots or notes of all pages with custom configurations. |
| 3 | Backup the 4.1 configuration to a safe location. |
| 4 | (Optional) The Dell OptiPlex XE models of the NVR have an internal NIC card fitted to one of the units PCI slots. This card should be removed by a competent installer prior to commencing the upgrade. Once the card is removed the client network cable should be inserted into NIC1 and the camera network cable inserted into NIC2 on the unit. |
| 5 | Restart the system. |
| 6 | The NVR boots from the disk or USB drive and the installation options menu opens. |

**Note**

If the NVR does not boot from the software CD or USB drive, you will need to enter the BIOS Manager and Confirm that the 1st Boot Device is CD/DVD or Alternative Hard Disk (USB). Refer to Procedure 3-4 Verify BIOS Configuration on page 11.

| | |
|---|---|
| 7 | From the installations option menu select **NVR Live Installer**. |

**Note**

After approximately 20 seconds the installation will automatically start in this mode.

A Loading Linux Kernel pop up displays followed by a series of boot messages. This process may take several minutes.

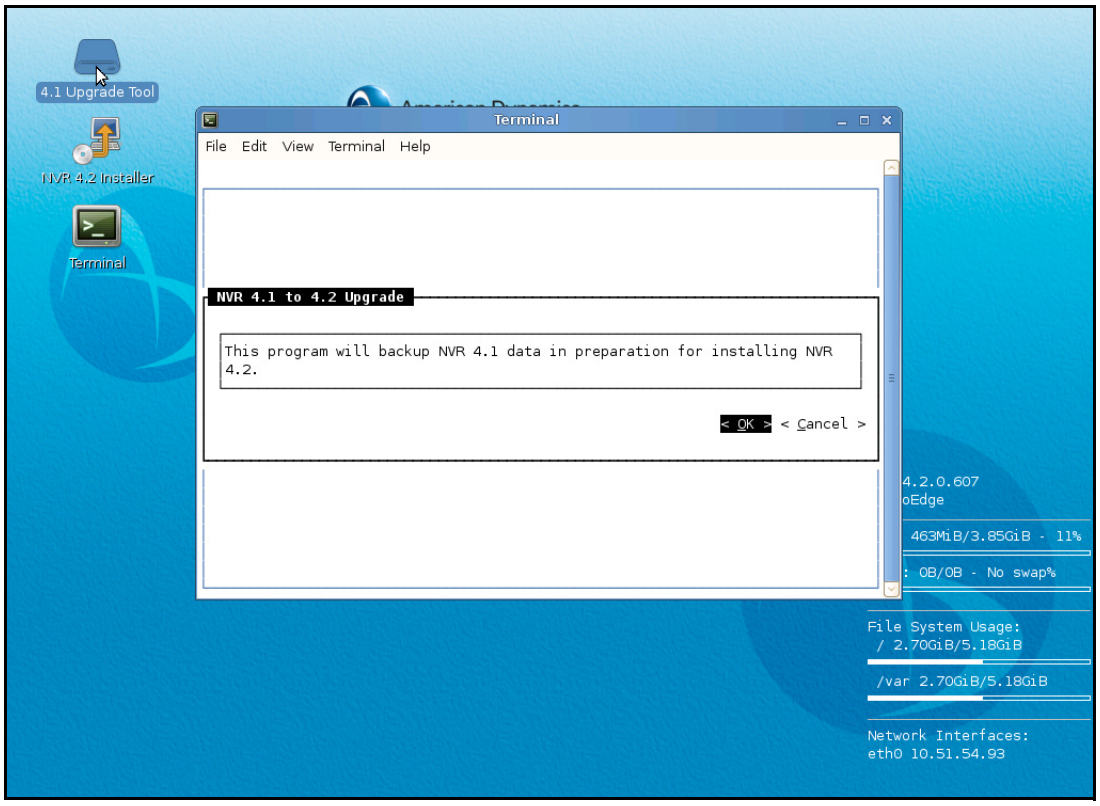
When the system has finished booting a desktop opens with three icons; the NVR Installation tool, the NVR Upgrade tool and Terminal.

| | |
|---|---|
| 8 | Double-click the **4.1 Upgrade Tool** icon to launch the upgrade tool. |

### Figure 26-2 4.1 Upgrade Tool

The Linux Terminal pop-up window opens displaying the upgrade wizard. Continue to Using the 4.1 Upgrade Tool to Launch the YaST Wizard on page 282.

**Figure 26-3 Upgrade Wizard**




**- End -**

## Caution

This is the last stage that it is still possible to revert back to the 4.1 software. Clicking Install will initiate the installation.

## Using the 4.1 Upgrade Tool to Launch the YaST Wizard

The 4.1 Upgrade Tool will guide you through the first stage of the upgrade process and initialise the second stage. When the second stage is initialized the YaST wizard will launch to configure your NVR's settings.

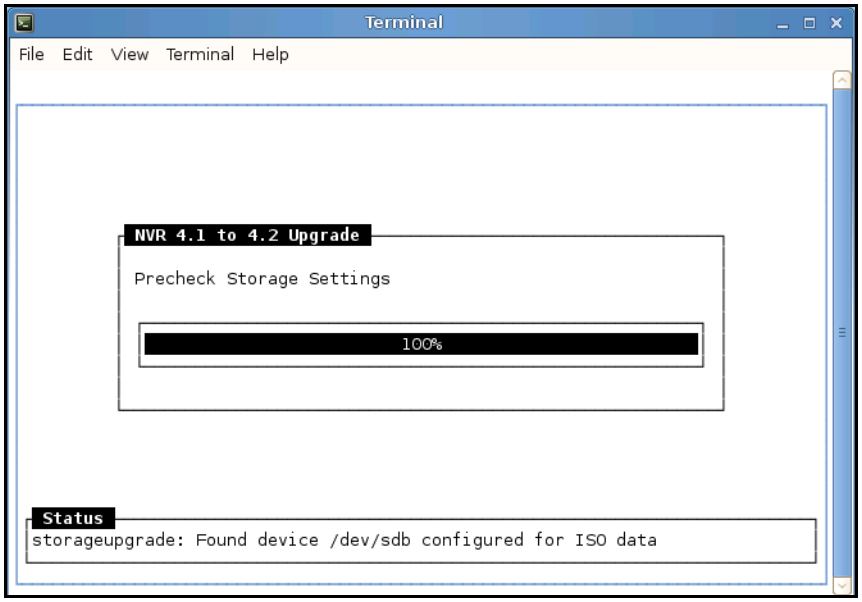
### Procedure 26-4
### Using the 4.1 Upgrade Tool to Launch the YaST Wizard

| Step | Action |
|---|---|
| 1 | Use the arrow keys to highlight **OK**, press the **[Return]** key.<br>This will initiate the first stage of the upgrade; Backup of the 4.1 application and OS settings. |

The upgrade tool will pre-check that it can restore the NVR 4.1 IP addresses and connect to any external storage devices, for example iSCSI drives.

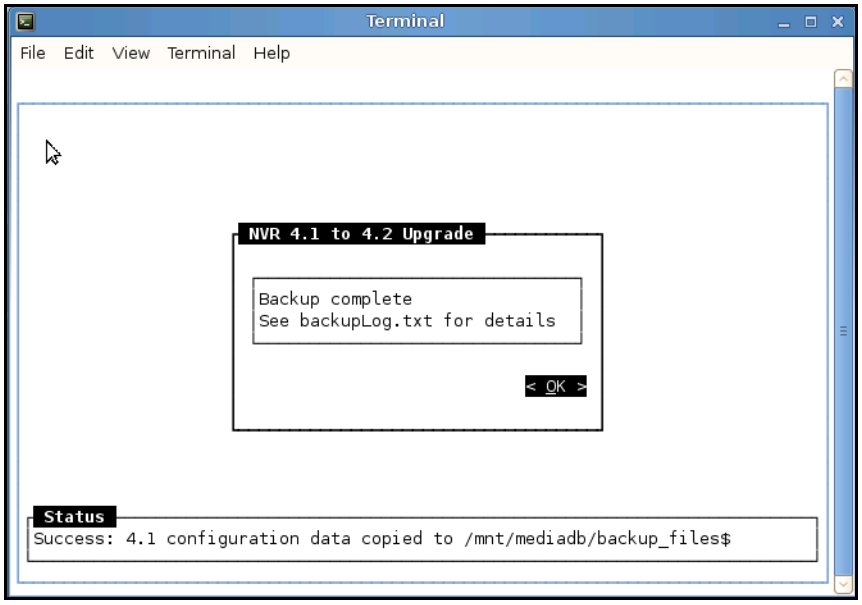
A progress bar will display percentage completion of the pre-check process.

**Figure 26-4 Backup Progress Bar**




2 Once complete a Backup Complete message will display. Press the **[Return]** key to initiate the second stage of the upgrade process: Installation of NVR 4.2.1 Software.

**Figure 26-5 Backup Complete**

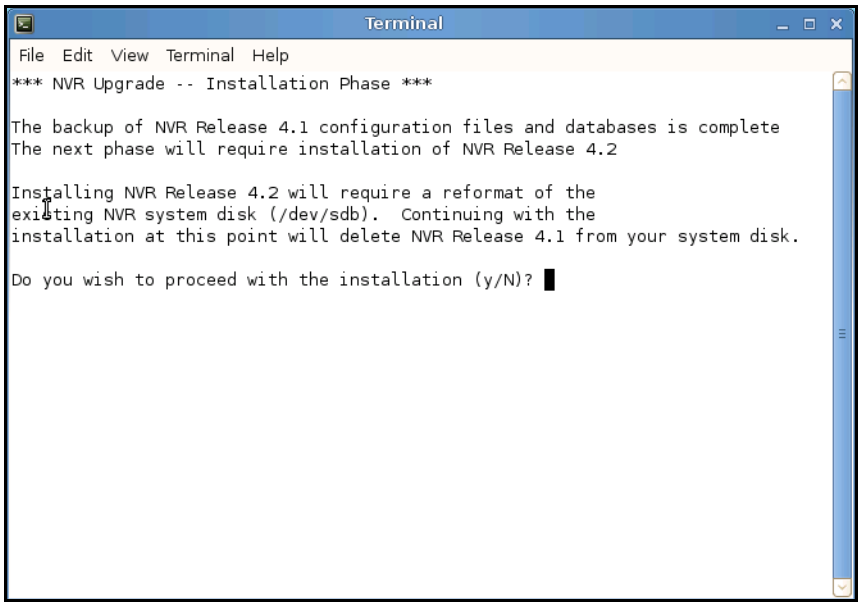



3 A warning message displays before launching the second stage. To continue enter **Y** followed by the **[Return]** key.

If you abort the upgrade at this point, you can remove the software CD/USB drive and reboot the NVR. Your 4.1 software will open as before.

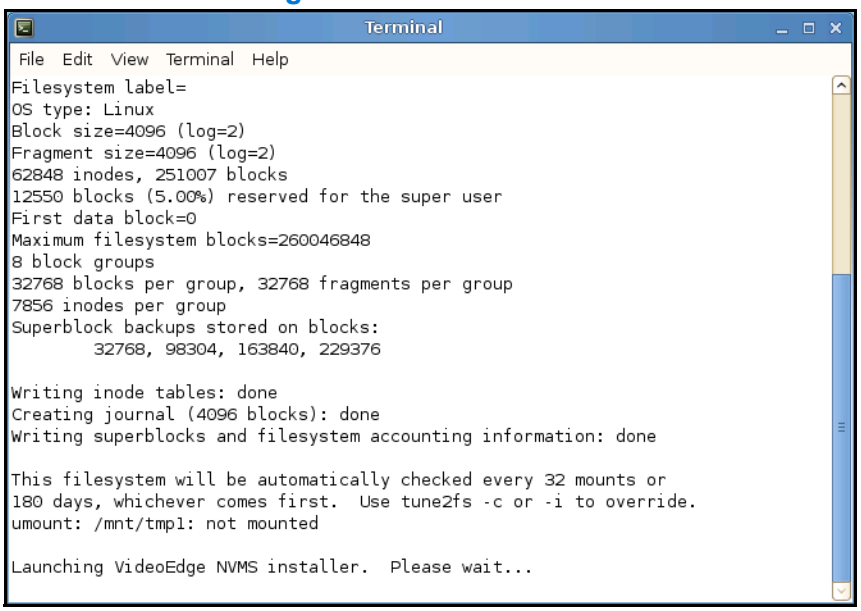
If you continue to progress with the upgrade you will be unable to roll back the software to 4.1 without encountering issues.

**Figure 26-6 Proceed with Install**


Terminal
File Edit View Terminal Help
*** NVR Upgrade -- Installation Phase ***
The backup of NVR Release 4.1 configuration files and databases is complete
The next phase will require installation of NVR Release 4.2
Installing NVR Release 4.2 will require a reformat of the
existing NVR system disk (/dev/sdb). Continuing with the
installation at this point will delete NVR Release 4.1 from your system disk.
Do you wish to proceed with the installation (y/N)?

The Live Installer launches.

**Figure 26-7 Live Installer**


Terminal
File Edit View Terminal Help
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
62848 inodes, 251007 blocks
12550 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=260046848
8 block groups
32768 blocks per group, 32768 fragments per group
7856 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 32 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
umount: /mnt/tmp1: not mounted
Launching VideoEdge NVMS installer. Please wait...

The YaST Installation wizard launches.

**- End -**

## Using the YaST Wizard

During the second stage of the upgrade process the YaST wizard launches. The YaST wizard is used to configure your NVR's settings including; language, keyboard layout, date and time and partitioning. Once the YaST wizard is complete the final stage of the upgrade process is initialized, reopening the upgrade tool.

## Procedure 26-5
## Using the YaST Wizard

| Step | Action |
|---|---|

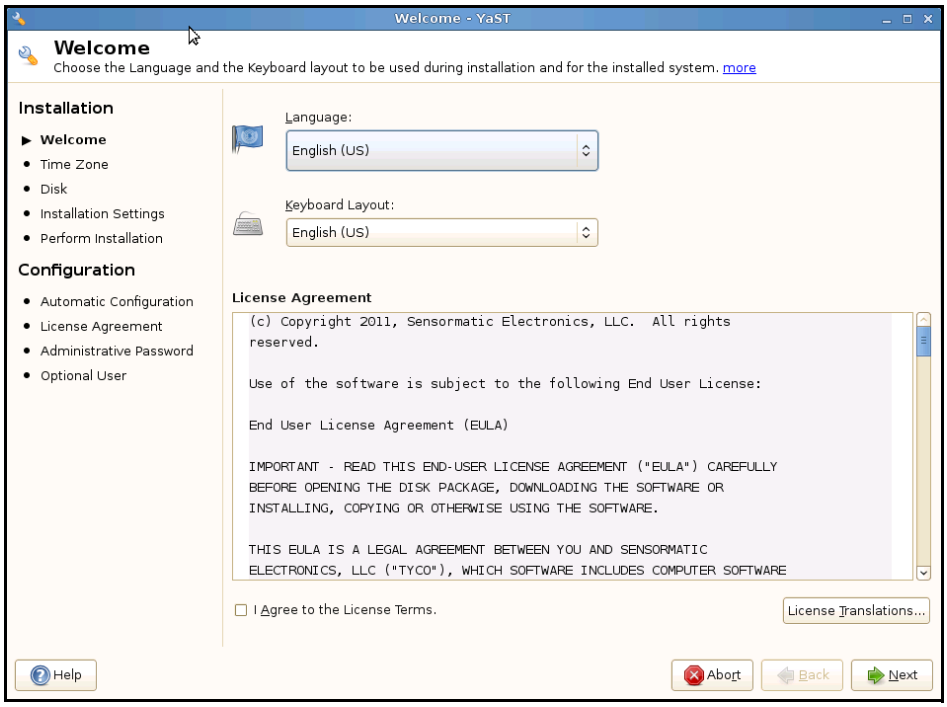
1 Select the required **Language** from the dropdown.

2 Select the **Keyboard Layout** from the dropdown.

3 (Optional) Click the **License Translations...** button to view the license in a different language.

4 After reading the licence agreement, select the **I Agree to the License Terms** checkbox.

**Figure 26-8 Welcome Page**


Welcome - YaST
Welcome
Choose the Language and the Keyboard layout to be used during installation and for the installed system. more
Installation
Welcome
Time Zone
Disk
Installation Settings
Perform Installation
Configuration
Automatic Configuration
License Agreement
Administrative Password
Optional User
Language:
English (US)
Keyboard Layout:
English (US)
License Agreement
(c) Copyright 2011, Sensormatic Electronics, LLC. All rights reserved.
Use of the software is subject to the following End User License:
End User License Agreement (EULA)
IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.
THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE
I Agree to the License Terms.
License Translations...
Help
Abort
Back
Next

5 Click **Next**.

The Clock and Time Zone page opens.

6 Select the **Region** from the dropdown.

7 Select the **Time Zone** from the dropdown.

The date and time for the selected time zone is displayed.

**Note**

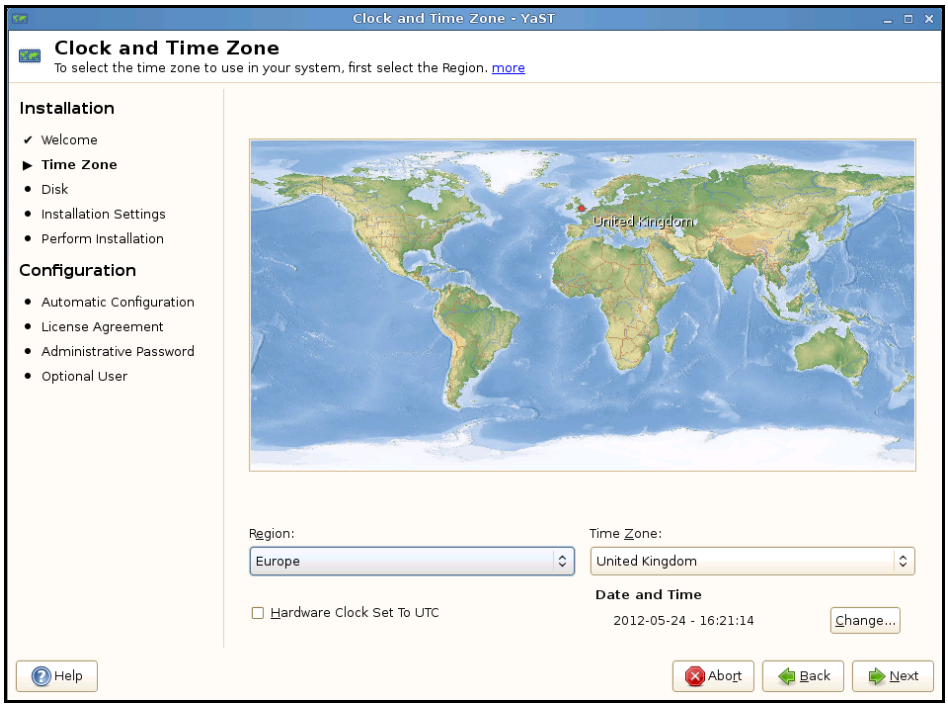
If the time and date settings are not correct you can manually update the settings by clicking the **Change...** button and manually entering the current date and time, or synchronize with the NTP server.

8 (Optional) Select the **Hardware Clock Set To UTC** checkbox.

**Note**

You should only select this checkbox if the systems hardware clock is set to UTC.

**Figure 26-9 Clock and Time Zone Page**




9 Click **Next**.

The Suggested Partitioning page opens.

10 Click the **Import Partition Setup...** button.

A popup window opens.

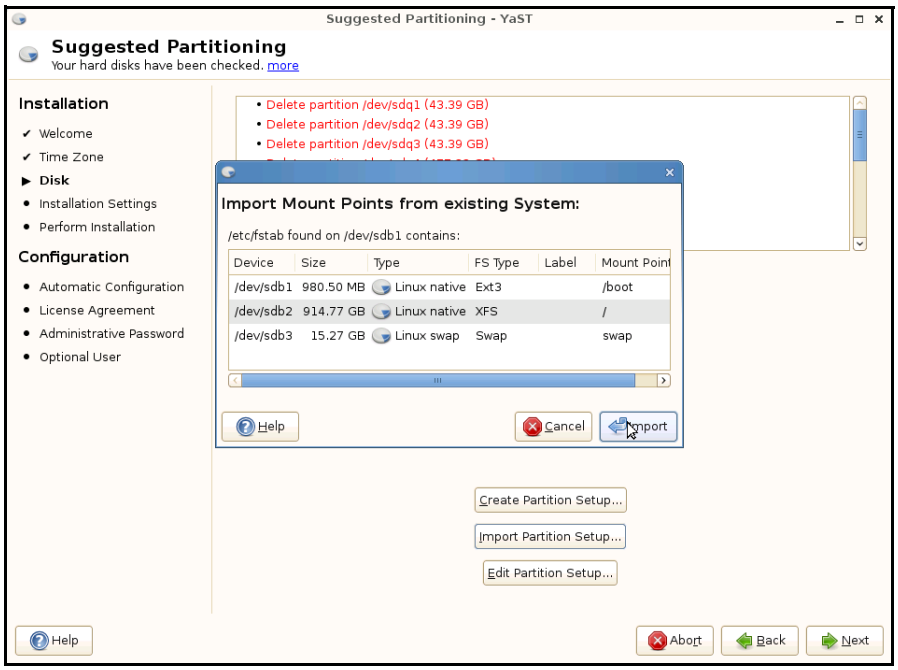
It is highly recommended at this point you identify the boot disk. This is the disk containing the partitions **swap**, **/** and **/var**. In the example below the imported partitions belong to disk; /dev/sdb1. Take note of the boot disk in your case, depending on your system you may need this information during the Installation Settings phase.

11 Click the **Import** button.

## Caution

To access recorded media from your NVR 4.1 you must import the partition setup. Failure to do so will result in the loss of previously recorded media.

**Figure 26-10 Suggested Partitioning Page**




**12** Click **Next**.

The Live Installation Settings page displays. This provides a summary of the 4.2.1 installation.

**Note**

For NVR systems with a large number of external disks you may see the following error:

'Configure a valid boot loader location before continuing.'

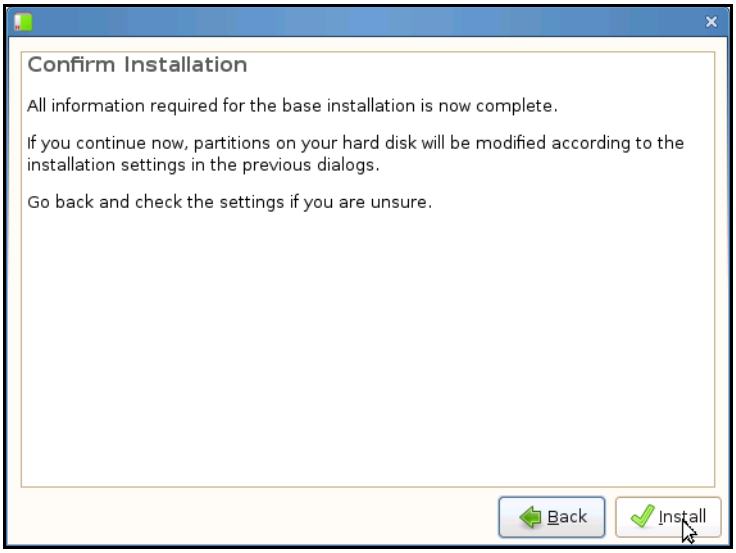
The device map includes more than 8 devices and the boot device is out of range. The range is limited by BIOS to the first 8 devices.

For further information refer to Procedure 26-7 Changing the Disk Boot Order during Live Installer on page 292.

**13** Click **Install**.

A popup window opens asking you to confirm installation.

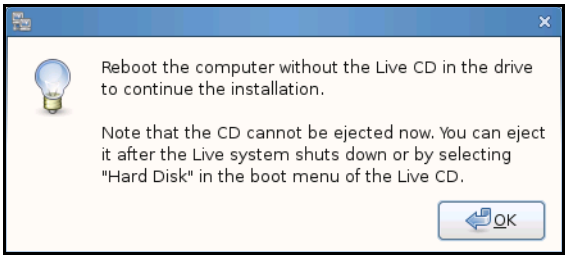
**Figure 26-11 Confirm Installation Popup**


Confirm Installation
All information required for the base installation is now complete.
If you continue now, partitions on your hard disk will be modified according to the installation settings in the previous dialogs.
Go back and check the settings if you are unsure.
Back
Install

**14** Click **Install**.

**15** The installation process begins. A progress bar is displayed at the bottom of the page. Once Installation is complete a popup window opens prompting you to reboot the computer.

**Figure 26-12 Reboot Popup**


Reboot the computer without the Live CD in the drive to continue the installation.
Note that the CD cannot be ejected now. You can eject it after the Live system shuts down or by selecting "Hard Disk" in the boot menu of the Live CD.
OK

**16** Click **OK**.

The YaST Wizard closes and prior to rebooting the upgrade tool reopens.

**- End -**

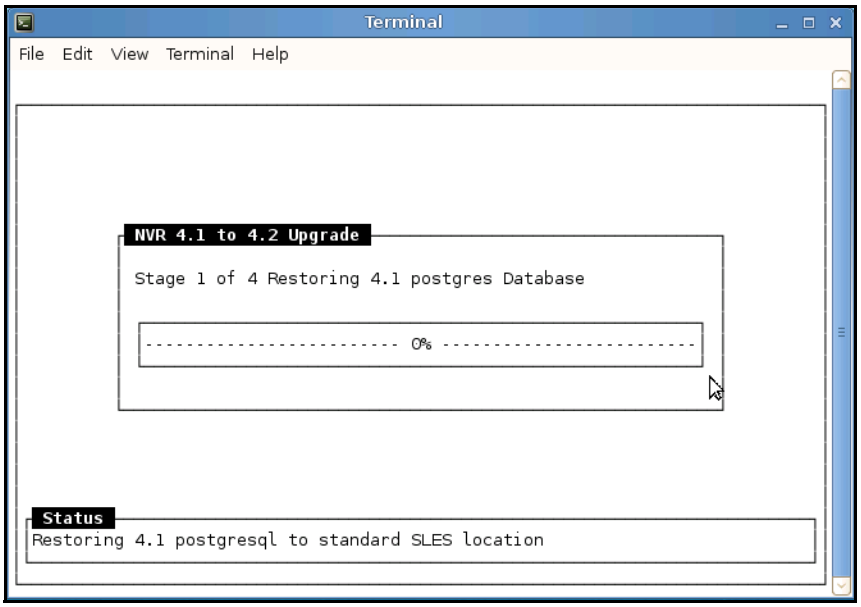
## Completing the Upgrade

Once the YaST wizard has closed the upgrade tool automatically reopens and commences the final stage of the upgrade, restoring NVR 4.1 application and OS settings including camera settings, media database, alarms, storage settings and network settings.

### Procedure 26-6
### Completing the Upgrade

| Step | Action |
|---|---|
| **1** | A progress bar will display the percentage completion of the restoration process. |

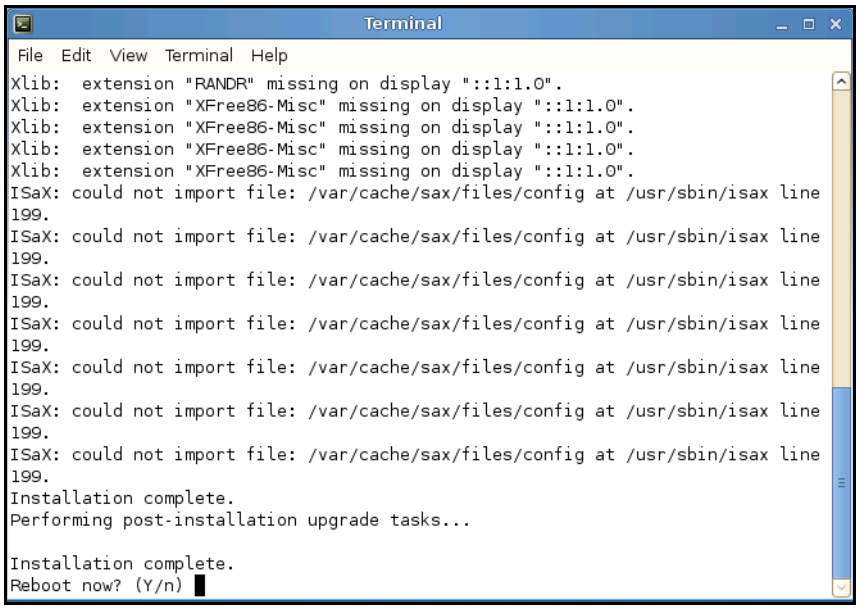
### Figure 26-13 Restoration Progress Bar


Terminal
File Edit View Terminal Help
NVR 4.1 to 4.2 Upgrade
Stage 1 of 4 Restoring 4.1 postgres Database
---------- 0% ----------
Status
Restoring 4.1 postgresql to standard SLES location

2 Once the restoration is complete, press the **[Return]** key.

Terminal displays 'Installation complete. Reboot now? (Y/n).

### Figure 26-14 Installation Complete. Reboot Now?


Terminal
File Edit View Terminal Help
Xlib: extension "RANDR" missing on display "::1:1.0".
Xlib: extension "XFree86-Misc" missing on display "::1:1.0".
Xlib: extension "XFree86-Misc" missing on display "::1:1.0".
Xlib: extension "XFree86-Misc" missing on display "::1:1.0".
Xlib: extension "XFree86-Misc" missing on display "::1:1.0".
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
ISaX: could not import file: /var/cache/sax/files/config at /usr/sbin/isax line 199.
Installation complete.
Performing post-installation upgrade tasks...
Installation complete.
Reboot now? (Y/n)

3 Enter **Y** followed by the **[Return]** key.

The NVR reboots.

4 When the NVR has restarted and the BIOS prompt displays you should remove the software CD/USB drive.

**Note**

If you accidently reboot the NVR and do not remove the software CD/USB you should reboot again and remove the CD/USB when the BIOS prompt displays.

5 The NVR will load to the License agreement and user accounts page. For further information refer to Procedure 3-10 Rebooting the NVR After Basic Installation on page 21.

6 Log in to the Linux OS of the NVR using the **root** user account.

7 Select the **VideoEdge Administrator** icon.

**Figure 26-15 VideoEdge Administrator Icon**

8 You will be prompted to enter a Username and Password. Enter the following credentials:

Username: **admin**

Password: **VIDEO!edge23**

9 Click **OK**.

The Setup Wizard's Welcome page opens.

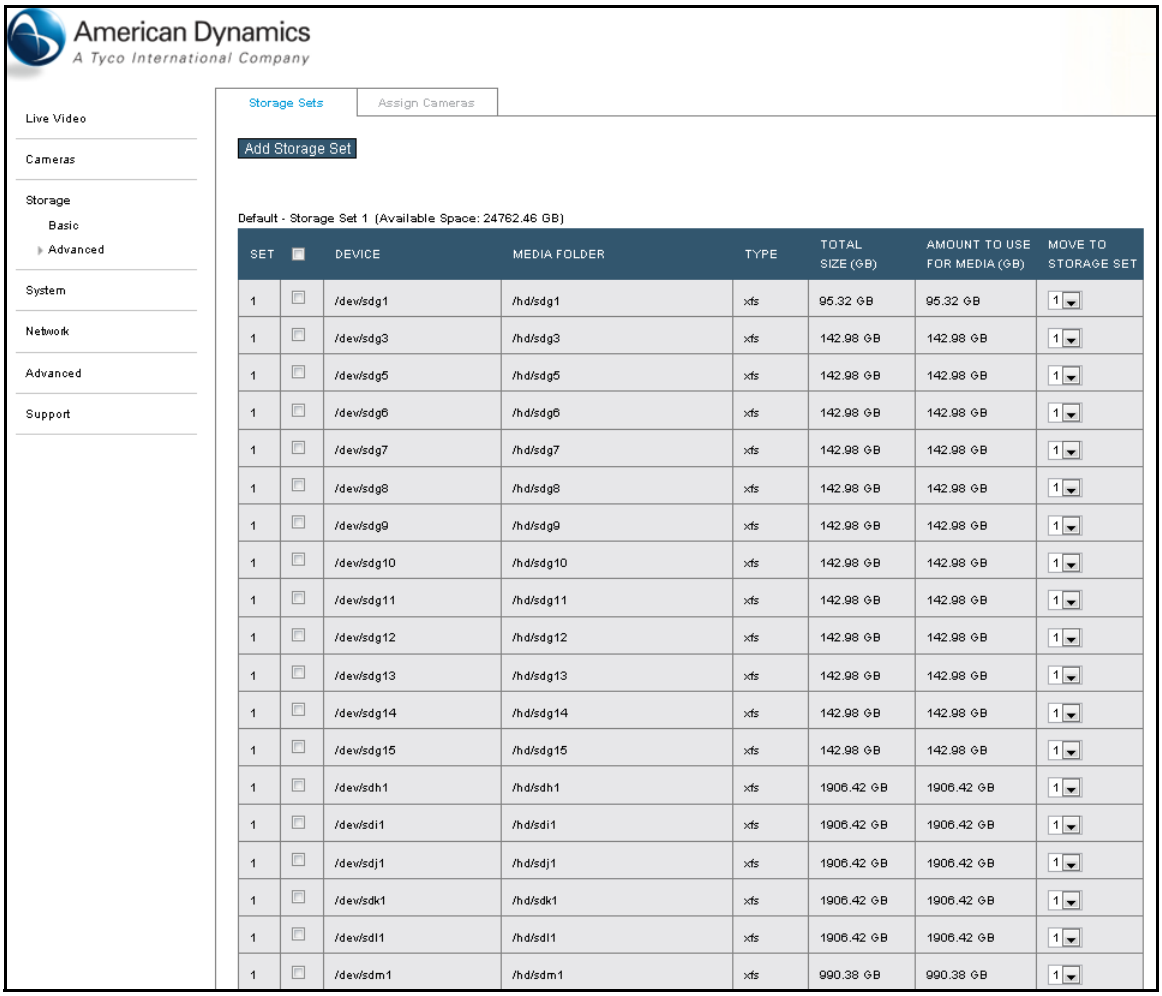
10 Complete the Setup Wizard. For further information refer to VideoEdge Setup Wizard on page 25.

NVR 4.1 settings will already be implemented as you progress through the Setup Wizard. Verify these previous NVR settings and configure any new settings which are available on the NVR 4.2.1 software that the wizard may prompt for.

The storage partitions from your 4.1 NVR are transferred to your 4.2.1 NVR and assigned to the same storage set. In the storage configuration pages all media folders apart from one will have the same name as was used in the 4.1 partition appended by the number '1'. For example, 4.1 partitions sdh and sdj will be named sdh1 and sdj1 on your NVR 4.2.1.

One partition from your 4.1 unit is divided into 14 smaller partitions. Thirteen of these partitions are available as media folders and can be used to store media. One partition is reserved as the clip export partition. The 13 media folders that are available for storage have the 4.1 partition name appended with numbers 1-15, excluding numbers 2 and 4. For example, if the partition was named in the 4.1 NVR as sdg, in your NVR 4.2.1 the 13 smaller partitions representing this larger partition are named, sdg1, sdg3, sdg5 up to sdg15. The partitions appended by numbers 2 and 4 are not visible in the storage configuration pages, as number 2 is used by the clip export partition and number 4 is utilized by the NVR as part of the partition method. Figure 26-16 below shows the upgraded storage media folders.

**Figure 26-16 Upgraded Storage**


American Dynamics
A Tyco International Company
Live Video
Cameras
Storage
Basic
Advanced
System
Network
Advanced
Support
Storage Sets
Assign Cameras
Add Storage Set
Default - Storage Set 1 (Available Space: 24762.46 GB)
SET
DEVICE
MEDIA FOLDER
TYPE
TOTAL SIZE (GB)
AMOUNT TO USE FOR MEDIA (GB)
MOVE TO STORAGE SET
1 /dev/sdg1 /hd/sdg1 xfs 95.32 GB 95.32 GB 1
1 /dev/sdg3 /hd/sdg3 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg5 /hd/sdg5 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg6 /hd/sdg6 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg7 /hd/sdg7 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg8 /hd/sdg8 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg9 /hd/sdg9 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg10 /hd/sdg10 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg11 /hd/sdg11 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg12 /hd/sdg12 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg13 /hd/sdg13 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg14 /hd/sdg14 xfs 142.98 GB 142.98 GB 1
1 /dev/sdg15 /hd/sdg15 xfs 142.98 GB 142.98 GB 1
1 /dev/sdh1 /hd/sdh1 xfs 1906.42 GB 1906.42 GB 1
1 /dev/sdi1 /hd/sdi1 xfs 1906.42 GB 1906.42 GB 1
1 /dev/sdj1 /hd/sdj1 xfs 1906.42 GB 1906.42 GB 1
1 /dev/sdk1 /hd/sdk1 xfs 1906.42 GB 1906.42 GB 1
1 /dev/sdl1 /hd/sdl1 xfs 1906.42 GB 1906.42 GB 1
1 /dev/sdm1 /hd/sdm1 xfs 990.38 GB 990.38 GB 1

All camera settings are transferred to the NVR 4.2.1 and cameras are assigned to the same storage sets.

When the wizard is complete, the NVR Configuration interface opens. All settings configured are available to edit if required.

**- End -**

## Changing the Disk Boot Order

When upgrading NVR systems with large numbers of connected iSCSI disks it is necessary to ensure that the boot disk is a position less than number 8 in the device list.The NVR BIOS is only able to boot from one of the first eight disks.

### Procedure 26-7 Changing the Disk Boot Order during Live Installer

| Step | Action |
|---|---|
| 1 | In the installation summary page, click **Change** and select **Booting...**.<br>The Boot Loader Settings page opens. |
| 2 | Select the **Boot Loader Installation** tab. |
| 3 | Click **Boot Loader Installation Details**. |
| 4 | Locate the **boot disk** and select it.<br>The boot disk will be highlighted once selected.<br>**Note**<br>You should have noted the disk ID of the book disk earlier in step 11 of Procedure 26-5 Using the YaST Wizard on page 285. If not you can read the file in '/tmp/migration/nvr-system-disk-setup/'. It is detailed in the line 'system-disk=...'. |
| 5 | Click **Up** until the boot disk is in positioned less than number 8 in the device list. |
| 6 | Click **OK**. |
| 7 | Select **Boot from Boot Partition**, deselect any other selected options. |
| 8 | Click **OK**. |
| 9 | Click **Install** to proceed with the installation. |

**- End -**

# NVR 4.1 to 4.2.1 Migration Failure Recovery

Should a failure arise during the upgrade or migration process, the following procedure can be used to rollback your NVR to version 4.1.

To carry out the rollback procedure you will require the following:

1. A system backup file (from **NVR 4.1 only**). The backup file must consist of all cameras recording mode set to **OFF**.
2. NVR 4.1 Software CD or USB drive.

Video of previously archived alarms are not removed during reindex, so the archive partition will contain data under a directory called CamFolder instead of CamArchive. The CamArchive directory was renamed to CamFolder during the upgrade to 4.2.1.

The following items are not recovered during this rollback procedure:

- Alarm sensor configuration
- Previous event information
- Custom users and user roles

- Events.

**Note**

After the 4.2.1 upgrade has been completed, a rollback to version 4.1 will be treated as a system disk crash. All of the limitations of a system disk crash recovery will apply.

## Procedure 26-8
## NVR 4.1 to 4.2.1 Migration Failure Recovery

| Step | Action |
|---|---|
| 1 | Insert the NVR 4.1 software CD into the optical drive. |
| 2 | Reboot the NVR. |
| 3 | Boot from the NVR 4.1 software CD or USB drive. |
| 4 | Ensure that external connections are present. |
| 5 | Complete the installation process. |
| 6 | Apply the NVR License. |
| 7 | Restore the system backup file. |
| 8 | Reindex media data using the web client (http://<NVR-IP-Address>/admin-cgi/mediadbReindexer). |
| 9 | Recover procedure is complete and you can confirm as necessary. |

**- End -**

# End User License Agreement (EULA)

IMPORTANT - READ THIS END-USER LICENSE AGREEMENT ("EULA") CAREFULLY BEFORE OPENING THE DISK PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE.

THIS EULA IS A LEGAL AGREEMENT BETWEEN YOU AND SENSORMATIC ELECTRONICS, LLC ("TYCO"), WHICH SOFTWARE INCLUDES COMPUTER SOFTWARE AND MAY INCLUDE MEDIA, PRINTED MATERIALS, AND "ON-LINE" OR ELECTRONIC DOCUMENTATION (COLLECTIVELY, THE "SOFTWARE"). BY BREAKING THE SEAL ON THIS PACKAGE, DOWNLOADING THE SOFTWARE OR INSTALLING, COPYING OR OTHERWISE USING THE SOFTWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS EULA, DO NOT OPEN, DOWNLOAD, INSTALL, COPY OR OTHERWISE USE THE SOFTWARE.

1. SCOPE OF LICENSE. The Software may include computer code, program files and any associated media, hardware or software keys, printed material and electronic documentation. The Software may be provided to you pre-installed on a storage device (the media) as part of a computer system or other hardware or device ("System"). The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Tyco and/or its suppliers. The Software is licensed, not sold. All rights not expressly granted under this EULA are reserved by Tyco and its suppliers.

2. GRANT OF LICENSE. This EULA grants you the following rights on a non-exclusive basis:

a. General. This EULA permits you to use the Software for which you have purchased this EULA. Once you have purchased licenses for the number of copies of the Software that you require, you may use the Software and accompanying material provided that you install and use no more than the licensed number of copies at one time. The Software is only licensed for use with specified Licensor-supplied Systems. If the Software is protected by a software or hardware key or other device, the Software may be used on any computer on which the key is installed. If the key locks the Software to a particular System, the Software may only be used on that System.

b. Locally Stored Components. The Software may include a software code component that may be stored and operated locally on one or more devices. Once you have paid the required license fees for these devices (as determined by Tyco in its sole discretion), you may install and/or use one copy of such component of the Software on each of the devices as licensed by Tyco. You may then use, access, display, run or otherwise interact with ("use") such component of the Software in connection with operating the device on which it is installed solely in the manner set

forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software.

c. Remotely Stored Components. The Software may also include a software code component for operating one or more devices remotely. You may install and/or use one copy of such component of the Software on a remote storage device on an internal network with all of the devices and may operate such component with each device over the internal network solely in the manner set forth in any accompanying documentation or, in the absence of such, solely in the manner contemplated by the nature of the Software; provided however, you must still acquire the required number of licenses for each of the devices with which such component is to be operated.

d. Embedded Software/Firmware. The Software may also include a software code component that is resident in a device as provided by Tyco for operating that device. You may use such component of the Software solely in connection with the use of that device, but may not retrieve, copy or otherwise transfer that software component to any other media or device without Tyco's express prior written authorization.

e. Backup Copy. You may make a back-up copy of the Software (other than embedded software) solely for archival purposes, which copy may only be used to replace a component of the Software for which you have current valid license. Except as expressly provided in this EULA, you may not otherwise make copies of the Software, including the printed materials.

3. OTHER RIGHTS AND LIMITATIONS. Your use of the Software is subject to the following additional limitations. Failure to comply with any of these restrictions will result in automatic termination of this EULA and will make available to Tyco other legal remedies.

a. Limitations on Reverse Engineering and Derivative Works. You may not reverse engineer, decompile, or disassemble the Software, and any attempt to do so shall immediately terminate this EULA - except and only to the extent that such activity may be expressly permitted by applicable law notwithstanding this limitation. You may not make any changes or modifications to any portion of the Software, or create any derivative works, without the written permission of an officer of Tyco (except as provided in Section 3(f) of this EULA with respect to "open source" software). You may not remove any proprietary notices, marks or labels from the Software. You shall institute reasonable measures to ensure compliance with the terms and conditions of this EULA by your personnel and agents.

b. Copyright Notices. You must maintain all copyright notices on all copies of the Software.

c. Transfer. You may only transfer your rights under this EULA (i) as part of a permanent sale or transfer of all of the devices for which the Software is licensed as applicable; (ii) if you transfer all of the Software (including all component parts, the media and printed materials, any upgrades and this EULA); (iii) if you do not retain any copies of any portion of the Software; (iv) if the recipient agrees to the terms of this EULA; and (v) if the Software is an upgrade, such transfer must also include all prior versions of the Software. You agree that failure to meet all of these conditions renders such transfer null and void.

d. Termination.Without prejudice to any other rights, Tyco may terminate this EULA if you fail to comply with the terms and conditions herein. In such event, you must immediately destroy all copies of the Software and all of its component parts. To the extent the Software is embedded in hardware or firmware, you will provide prompt access to Tyco or its representative to remove or lock Software features or functionality as Tyco determines.

e. Subsequent EULA. Tyco may also supersede this EULA with a subsequent EULA pursuant to providing you with any future component, release, upgrade or other modification or addition to the Software. Similarly, to the extent that the terms of this EULA conflict with any prior EULA or other agreement between you and Tyco regarding the Software, the terms of this EULA shall prevail.

f. Incorporation of "Open Source" and other Third Party Software. Portions of the Software may be subject to certain thirty party license agreements governing the use, copying, modification, redistribution and warranty of those portions of the Software, including what is commonly known as "open source" software. A copy of each applicable third party license can be found in the file README.TXT or other documentation accompanying the Software. By using the Software you are also agreeing to be bound to the terms of such third party licenses. If provided for in the applicable third party license, you have a right to receive source code for such software for use and distribution in any program that you create, so long as you in turn agree to be bound to the terms of the applicable third party license, and your programs are distributed under the terms of that license. A copy of such source code may be obtained free of charge by contacting your Tyco representative.

g. Trademarks. This EULA does not grant you any rights in connection with any trademarks or service marks of Tyco, its affiliates or its suppliers.

h. Rental. You may not sublicense, rent, lease or lend the Software. You may not make it available to others or post it on a server or web site or otherwise distribute it.

i. Software Keys. The hardware/software key, where applicable, is your proof of license to exercise the rights granted herein and must be retained by you. Lost or stolen keys will not be replaced.

j. Demonstration and Evaluation Copies. A demonstration or evaluation copy of the Software is covered by this EULA; provided that the licenses contained herein shall expire at the end of the demonstration or evaluation period.

k. Registration of Software. The Software may require registration with Tyco prior to use. If you do not register the Software, this EULA is automatically terminated and you may not use the Software.

l. Additional Restrictions. The Software may be subject to additional restrictions and conditions on use as specified in the documentation accompanying such Software, which additional restrictions and conditions are hereby incorporated into and made a part of this EULA.

m. Upgrades and Updates. To the extent Tyco makes them available, Software upgrades and updates may only be used to replace all or part of the original Software that you are licensed to use. Software upgrades and updates do not increase the number of copies licensed to you. If the Software is an upgrade of a component of a package of Software programs that you licensed as a single product, the Software may be used and transferred only as part of that single product package and may not be separated for use on more than one computer or System. Software upgrades and updates downloaded free of charge via a Tyco authorized World Wide Web or FTP site may be used to upgrade multiple Systems provided that you are licensed to use the original Software on those Systems.

n. Tools and Utilities. Software distributed via a Tyco-authorized World Wide Web or FTP site (or similar Tyco-authorized distribution means) as a tool or utility may be copied and installed without limitation provided that the Software is not distributed or sold and the Software is only used for the intended purpose of the tool or utility and in conjunction with Tyco products. All other terms and conditions of this EULA continue to apply.

4. EXPORT RESTRICTIONS. You agree that you will not export, re-export or transfer any portion of the Software, or any direct product thereof (the foregoing collectively referred to as the "Restricted Components"), to IRAN, NORTH KOREA, SYRIA, CUBA and SUDAN, including any entities or persons in those countries, either directly or indirectly ("Tyco's Position"). You also agree that you will not export, re-export or transfer the Restricted Components to any other countries except in full compliance with all applicable governmental requirements, including but not limited to applicable economic sanctions and constraints administered by the U.S. Treasury Department and applicable export control measures administered by the U.S. Department of Commerce and U.S. Department of State, any other U.S. government agencies, and measures administered by the European Union or the government agencies of any other countries. Any violation by you of the applicable laws or regulations of the U.S. or any other government, or where you breach Tyco's Position notwithstanding whether or not this is contrary to any aforementioned applicable laws or regulations, will result in automatic termination of this EULA.

5. U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is Commercial Computer Software provided with "restricted rights" under Federal Acquisition Regulations and agency supplements to them. Any use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFAR 255.227-7013 et. seq. or 252.211-7015, or subparagraphs (a) through (d) of the Commercial Computer Software Restricted Rights at FAR 52.227-19, as applicable, or similar clauses in the NASA FAR Supplement. Contractor/manufacturer is Sensormatic Electronics, LLC, 6 Technology Park Drive, Westford, MA 01886.

6. LIMITED WARRANTY.

a. Warranty. Tyco warrants that the recording medium on which the Software is recorded, hardware key, and the documentation provided with it, will be free of defects in materials and workmanship under normal use for a period of ninety (90) days from the date of delivery to the first user. Tyco further warrants that for the same period, the Software provided on the recording medium under this license will substantially perform as described in the user documentation

provided with the product when used with specified hardware. THE FOREGOING EXPRESS WARRANTY REPLACES AND IS IN LIEU OF ALL OTHER WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING BUT NOT LIMITED TO, ANY IMPLIED OR OTHER WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OR NON-MISAPPROPRIATION OF INTELLECTUAL PROPERTY RIGHTS OF A THIRD PARTY, CUSTOM, TRADE, QUIET ENJOYMENT, ACCURACY OF INFORMATIONAL CONTENT, OR SYSTEM INTEGRATION. TYCO MAKES NO WARRANTY THAT ANY PORTION OF THE SOFTWARE WILL OPERATE ERROR-FREE, FREE OF ANY SECURITY DEFECTS OR IN AN UNINTERRUPTED MANNER. TYCO SHALL NOT BE RESPONSIBLE FOR PROBLEMS CAUSED BY CHANGES IN THE OPERATING CHARACTERISTICS OF THE DEVICE(S) UPON WHICH THE SOFTWARE IS OPERATING, OR FOR PROBLEMS IN THE INTERACTION OF THE SOFTWARE WITH NON-TYCO SOFTWARE OR HARDWARE PRODUCTS. TYCO NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON PURPORTING TO ACT ON ITS BEHALF TO MODIFY OR TO CHANGE THIS WARRANTY, NOR TO ASSUME FOR IT ANY OTHER WARRANTY OR LIABILITY CONCERNING THIS SOFTWARE. THE WARRANTY MADE BY TYCO MAY BE VOIDED BY ABUSE OR MISUSE. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS UNDER MANDATORY LAW THAT VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

b. Exclusive Remedy. Tyco's entire liability and your exclusive remedy under the warranty set forth in this Section 6 will be, at Tyco's option, to (i) attempt to correct Software errors with efforts Tyco believes suitable to the problem, (ii) replace at no cost the recording medium, Software or documentation with functional equivalents as applicable, or (iii) refund a pro-rated portion of the license fee paid for such Software (less depreciation based on a five-year life expectancy) and terminate this EULA, provided, in each case, that Tyco is notified in writing of all warranty problems during the applicable warranty period. Any replacement item will be warranted for the remainder of the original warranty period. No remedy is provided for failure of the Software if such failure is the result of accident, abuse, alteration or misapplication with respect to the Software or any hardware on which it is loaded. Warranty service or assistance is provided at the original point of purchase.

7. LIMITATION OF LIABILITY & EXCLUSION OF DAMAGES.

a. LIMITATION OF LIABILITY. IN NO EVENT WILL TYCO'S AGGREGATE LIABILITY (INCLUDING, BUT NOT LIMITED TO, LIABILITY FOR NEGLIGENCE, STRICT LIABILITY, BREACH OF CONTRACT, MISREPRESENTATION AND OTHER CONTRACT OR TORT CLAIMS) ARISING FROM OR RELATED TO THIS EULA, OR THE USE OF THE SOFTWARE, EXCEED THE GREATER OF USD$5.00 OR THE AMOUNT OF FEES YOU PAID TO TYCO OR ITS RESELLER FOR THE SOFTWARE THAT GIVES RISE TO SUCH LIABILITY. BECAUSE AND TO THE EXTENT THAT SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSIONS OR LIMITATIONS OF LIABILITY ABOVE, THESE MAY NOT APPLY TO YOU.

b. EXCLUSION OF OTHER DAMAGES. UNDER NO CIRCUMSTANCES SHALL TYCO OR ANY OF ITS RESELLERS OR LICENSORS BE LIABLE FOR ANY OF THE FOLLOWING: (I) THIRD PARTY CLAIMS; (II) LOSS OR DAMAGE TO ANY SYSTEMS, RECORDS OR DATA, OR LIABILITIES RELATED TO A VIOLATION OF AN INDIVIDUAL'S PRIVACY RIGHTS; OR (III) INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, PUNITIVE, RELIANCE, OR COVER DAMAGES (INCLUDING LOST PROFITS AND LOST SAVINGS), IN EACH CASE EVEN IF TYCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ARE SOLELY RESPONSIBLE AND LIABLE FOR VERIFYING THE SECURITY, ACCURACY AND ADEQUACY OF ANY OUTPUT FROM THE SOFTWARE, AND FOR ANY RELIANCE THEREON. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE LIMITATION ON HOW LONG AN IMPLIED WARRANTY LASTS, SO SOME OF THE ABOVE LIMITATIONS MAY APPLY TO YOU ONLY TO THE EXTENT PERMITTED BY THOSE LAWS.

8. GENERAL. If any provision of this EULA is found to be unlawful, void, or for any reason unenforceable, then that provision shall be severed from this EULA and shall not affect the validity and enforceability of the remaining provisions. You should retain proof of the license fee paid, including model number, serial number and date of payment, and present such proof of payment when seeking service or assistance covered by the warranty set forth in this EULA. This EULA is governed by the laws of the State of New York, without regards to its conflicts of law principles. The parties hereby irrevocably agree that they submit themselves to the personal jurisdiction of the state and federal courts of New York for purposes of resolving any and all disputes arising under or related to these terms and conditions. The parties specifically exclude the application of the provisions of the United Nations Convention on Contracts for the International Sale of Goods.

# Index


## A

Adding
- cameras 80, 83

Alarms
- motion detection 106
- video intelligence 117

Alert Sensors
- configuration 99

Audit Trail 206

## B

Backup
- configuration 181

Best Practices
- motion detection 103
- video intelligence 114

## C

Camera
- adding to NVR 80, 83
- calibrating 69
- configuration (advanced) 89
- configuration (basic) 85
- configuration (batch) 86
- motion detection 104
- password groups 91, 131
- recording mode 95
- removing 82
- storage statistics 196
- video intelligence 113

Camera List 77
- filtering 79

Changing
- system ID 136

Configuration
- alert sensors 99
- backup 181
- camera (advanced) 89
- camera (basic) 85
- camera (batch) 86
- DHCP network settings 155
- failover 179
- network settings 147
- paging file 237
- restore 182
- storage 65
- storage device 60
- WAN settings 157

Configuring Sensors
- dry contact sensors 99

Connecting
- FRS/FES storage 228
- iSCSI storage 230

## D

Dark Image Detection 217
- Camera Loss Detection 218

Disabling
- failover 179

Displaying
- NVR camera summary 79

## E

Email Alerts 209
- camera disable 212
- enable/disable 212
- set up 210

## F

Failover 177
- configuration 179
- disabling 179

Filtering
- camera list 79

FRS/FES
connecting to NVR 228

## G

Groups
camera password 91, 131
deleting camera password 133

## I

Installation
VideoEdgeNVR 4.2 7
iSCSI
connecting to NVR 230

## L

Licensing 281
Listing
NVR cameras 79
Live Video
QuickTime viewer 75
viewing 74
Login
NVR configuration interface via victor 52
NVR webserver interface 51
Logs 199
alert 215
camera 204
camera connection errors 203
event 202
FTP log management 201
retrieving 199

## M

Motion Detection
alarms 106
best practices 103
disabling 106
enabling 104

## N

Navigation
main menu 57
tabs 57
Network
configuration 147
DHCP settings 155
WAN settings 157
NVR Services
restart 169
stop 170

## O

Operational Statistics 189

## P

Paging File Configuration 237
Password
changing admin password 31
deleting groups 133
password groups 91, 131
Prerequisite Software 237

## R

Rebooting 171
Recording
modes 95
schedule 123
Remote desktop 264
RDP 264
VNC 267
Requirements
prerequisite software 237
system 6
Restart NVR Services 169
Restore
configuration 182
factory default settings 172

## S

Set Up
email alerts 210
Statistics
disk activity 193
recording 190
recording performance 189
storage 194
storage device 195
storage per camera 195, 196
storage set 194
Stop NVR Services 170
Storage
calculating requirements 226
concepts 221
connecting devices 228, 230
data culling 63
device configuration (advanced) 65
device configuration (basic) 60
monitoring 67
sets 59, 225
types 222
vaulted media 64
Storage Sets
camera assignment 68
creating 67
deleting 70
media folder assignment 68
statistics 194
System
requirements 6
shutdown 171
System ID
changing 136

## T

Template
importing 186
saving 185

## V

Video Intelligence
alarms 117
best practices 114
disabling 116
enabling 115
VideoEdge NVR
login (victor) 52
login (web GUI) 51
reboot 171
shutdown 169, 171
Viewing
live video 74